Universidade Estadual de Campinas
FACULDADE DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO
DEPARTAMENTO DE TELEMÁTICA

Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais

Tese apresentada à Faculdade de Engenharia Elétrica e de Computação da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Doutor em Engenharia Elétrica

por

Clarice Dias de Albuquerque

Orientador: **Prof. Dr. Reginaldo Palazzo Júnior** FEEC/UNICAMP

Co-orientador: **Prof. Dr. Eduardo Brandani da Silva** DMA/UEM

Banca Examinadora:

Prof. Dr. Max Henrique Machado Costa (FEEC/UNICAMP)
Prof. Dr. Amir Ordacgi Caldeira (IFGW/UNICAMP)
Prof. Dr. Orlando Stanley Juriaans (IME/USP)
Prof. Dr. Marcelo Muniz Silva Alves (DEPARTAMENTO DE MATEMÁTICA/UFPR)

Campinas - SP
2009

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DA ÁREA DE ENGENHARIA E ARQUITETURA - BAE - UNICAMP

AL15a

Albuquerque, Clarice Dias de
Análise e construção de códigos quânticos topológicos sobre variedades bidimensionais / Clarice Dias de Albuquerque. --Campinas, SP: [s.n.], 2009.

Orientadores: Reginaldo Palazzo Júnior, Eduardo Brandani da Silva.
Tese de Doutorado - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação.

1. Teoria da codificação. 2. Geometria hiperbolica. 3. Teroia dos reticulados. I. Palazzo Júnior, Reginaldo. II. Silva, Eduardo Brandani da. III. Universidade Estadual de Campinas. Faculdade de Engenharia Elétrica e de Computação. IV. Título.

Título em Inglês: Construction of topological quantum codes on bidimensional manifolds
Palavras-chave em Inglês: Coding theory, Hyberbolic geometry, Lattice theory
Área de concentração: Telecomunicações e Telemática
Titulação: Doutor em Engenharia Elétrica
Banca examinadora: Max Henrique Machado Costa, Amir Ordacgi Caldeira, Orlando Stanley Juriaans, Marcelo Muniz Silva Alves
Data da defesa: 03/04/2009
Programa de Pós Graduação: Engenharia Elétrica

COMISSÃO JULGADORA - TESE DE DOUTORADO

Candidata: Clarice Dias de Albuquerque

Data da Defesa: 3 de abril de 2009

Título da Tese: "Análise e Construção de Códigos Quânticos Topológicos sobre Variedades Bidimensionais"

Prof. Dr. Reginaldo Palazzo Júnior (Presidente): _____

Prof. Dr. Orlando Stanley Juriaans: _____

Prof. Dr. Marcelo Muniz Silva Alves: _____

Prof. Dr. Amir Ordacgi Caldeira: _____

Prof. Dr. Max Henrique Machado Costa: _____

Agradecimentos

A Deus, por tudo que me proporcionou, por todos os ensinamentos e todas as oportunidades, por ser meu guia e permitir-me conhecer tantas pessoas especiais ao longo da vida.

Ao meu orientador Reginaldo Palazzo Jr., uma pessoa admirável por sua educação, conhecimento, humildade e espírito desbravador que não teme novos caminhos, e a quem devo muito do que me tornei. Agradeço por ter acreditado em mim e orientado-me nesses anos sem deixar que eu perdesse o entusiasmo.

Ao meu amado marido, companheiro e melhor amigo Leandro (Du), por absolutamente tudo: seu amor, dedicação, carinho, cuidado, cumplicidade e otimismo. Por estar sempre ao meu lado, apoiando-me e me consolando. Sempre disposto a me ouvir e sem deixar que eu desanimasse. Sem ele seria impossível suportar tantas mudanças e saudades.

Aos meu pais Ronald e Conceição, a quem amo demais, pelo amor, dedicação, apoio e cuidado que sempre tiveram comigo. Sem dúvida, uma das piores dificuldades nesses quatro anos foi suportar a saudade que sinto deles, mas graças a tudo que me ensinaram consegui vencer mais uma etapa. Sinto imenso orgulho por tê-los como meus pais e meus primeiros e sempre orientadores.

Aos meus irmãos Ângela, Bartira e Ronald Filho, pelo incentivo, apoio e amor que sempre tiveram comigo. Sempre foi na minha família que consegui forças para continuar.

A tia Simone, a quem considero uma segunda mãe, o verdadeiro sentido de madrinha, por todo apoio e carinho.

A D. Ana, minha querida sogra, por acreditar em mim a ponto de deixar aos meu cuidados seu maior tesouro, seu filho Leandro. E aos meus cunhados Esio, Leo e Elisângela pelo carinho e atenção.

A todos os amigos do DT pelas boas conversas regadas a cafezinhos. Em especial ao Giuliano pela disponibilidade de assistir minhas apresentações e discutir os trabalhos, Renato e Ricardo pela ajuda com o Latex e outros assuntos computacionais, os colegas João Henrique, João Coelho, Júlio, Poliane e Ingrid, com quem dividi as aflições das disciplinas.

A todos os amigos do LTIA pela convivência: Daniel Chaves, Daniel Cunha, Rafael Mota, Rafael Marinho, Aido, Rodrigo, Manish e Vandenberg, especialmente as amigas Andrea, Cátia, Luzinete e Wanessa, por todas as conversas sérias ou não, pelos cafezinhos, e toda a diversão que foi conviver com elas esses anos.

Ao amigo Eduardo Brandani, pelos debates, discussões e momentos de descontração que tanto

contribuíram para esse trabalho.

Ao prof. Antônio Aparecido de Andrade pela ajuda e atenção.

Ao amigo PC por ter apresentado-me aos “códigos”. Aos professores Plácido, João de Deus, Luquésio e Trajano, por terem me possibilitado o contato com o professor Palazzo.

Aos primos Adriano pela atenção em rever alguns textos, e Salette pela ajuda e amizade.

A Flávia, Noêmia, Juraci, Soraia e Edson por toda ajuda, simpatia e competência.

Ao CNPQ pelo apoio financeiro fornecendo minha bolsa de estudos (140642/2005-6), e a FAPESP pelo suporte junto ao projeto temático 02/07473-7.

Aos membros da banca por aceitarem o convite, pela atenção dedicada a este trabalho, pelas sugestões e considerações.

A todos que, direta ou indiretamente, contribuíram para a conclusão deste trabalho.

Ao meu marido Leandro, e aos meus pais Ronald e Conceição por todo apoio e pelo amor que me ajuda a suportar e vencer barreiras.

É graça divina começar bem. Graça maior persistir na caminhada certa. Mas a graça das graças é não desistir nunca.

D. Hélder Câmara

O valor das coisas não está no tempo que elas duram, mas na intensidade com que acontecem.

Fernando Pessoa

Resumo

Neste trabalho apresentamos um amplo estudo de códigos quânticos topológicos, trazendo inovação para esta área. Inicialmente geramos novos códigos quânticos tóricos, dentre os quais se destaca a classe $[[d^2, 2, d]]$ cujos parâmetros são os melhores até então apresentados para este tipo de código. Nesta proposta sistematizamos a construção de códigos tóricos baseados em teoria de grupos e também em análise combinatória. Com respeito aos códigos quânticos topológicos em superfícies com gênero $g \geq 2$, apresentamos uma construção baseada em geometria hiperbólica, generalizando a construção de Kitaev. Reproduzimos e ampliamos a classe de códigos quânticos com distância 3 decorrentes de mergulhos de grafos completos em superfícies com gêneros específicos obtidos primeiramente por Bombin e Martin-Delgado, com o diferencial de descrevê-los geometricamente e exibir claramente seus parâmetros. Obtemos uma classe de códigos MDS (*Maximum Distance Separable*). Explicitamos em tabelas os melhores códigos para superfícies com gênero $g = 2, 3, 4$ e 5 obtidos a partir dessa construção, e analisamos esses resultados.

Palavras-Chave: códigos quânticos topológicos, códigos quânticos tóricos, códigos reticulados, códigos quânticos corretores de erros, códigos estabilizadores, códigos sobre superfícies.

Abstract

In this work we present an extensive study of topological quantum codes. As a consequence, new promising ideas, concepts and results are also presented. First of all, new toric quantum codes are constructed among which the $[[d^2,2,d]]$ class stands out as the best known so far. This proposed construction of toric codes is realized based upon group theory and combinatorial analysis. Regarding the topological quantum codes in surfaces with genus $g \geq 2$, we consider a construction method based on hyperbolic geometry and so generalizing Kitaev's construction. We reproduce and enlarge the class of quantum codes with distance 3 as a consequence of the embedding of complete graphs in surface with specific genus. This class was first proposed by Bombin and Martin-Delgado. The latter class is geometrically described and its parameters are explicitly exhibited. We also obtain a class of MDS (*Maximum Distance Separable*) codes in surfaces with genus $g = 2,3,4$ and 5, obtained by the proposed construction are tabulated and analyzed.

Key-words: topological quantum codes, toric quantum codes, lattice codes, error-correcting quantum codes, stabilizer codes, surface codes.

Conteúdo

Agradecimentos **i**

Dedicatória **iii**

Epígrafe **v**

Resumo **vii**

Abstract **ix**

Conteúdo **xi**

Lista de Figuras **xv**

Lista de Tabelas **xvi**

1 Introdução **1**

1.1 A Nova Teoria Física 2

1.1.1 A unidade de informação quântica 5

1.1.2 Vantagens que a mecânica quântica pode trazer para a computação 6

1.2 A Teoria dos Códigos Quânticos Corretores de Erros 7

1.3 Proposta da tese 8

1.4 Descrição da tese 9

2 Códigos Corretores de Erros Clássicos **11**

2.1 Códigos Corretores de Erros 11

2.2 Códigos de Bloco 15

2.2.1 Códigos lineares 16

2.2.2 Parâmetros de qualidade de um código 19

2.2.3 Exemplos de códigos de bloco 21

3 Códigos Quânticos Corretores de Erros **25**
3.1 Panorama Histórico . . . 25
3.2 Mecânica Quântica . . . 31
3.2.1 A propriedade da superposição . . . 32
3.2.2 A propriedade de emaranhamento . . . 35
3.3 Informação e Computação Quântica . . . 35
3.3.1 O bit quântico . . . 36
3.3.2 Álgebra linear . . . 38
3.3.3 Portas quânticas . . . 45
3.4 Códigos Quânticos Corretores de Erros . . . 47
3.4.1 Desafios conceituais . . . 48
3.4.2 O código de Shor . . . 49
3.4.3 Teoria quântica da correção de erro . . . 56
3.4.4 Códigos CSS . . . 60
3.5 Códigos Estabilizadores . . . 61

4 Códigos Quânticos Topológicos **69**
4.1 Código Tórico . . . 70
4.2 Computação Quântica Topológica . . . 75
4.2.1 Aspectos gerais de tolerância à falhas . . . 76
4.2.2 Anyons . . . 77
4.2.3 Computação anyônica . . . 79
4.3 Outros Códigos Quânticos Topológicos em Superfícies com Gênero $g = 0$ e $g = 1$ . . . 85
4.3.1 Códigos sobre o plano projetivo . . . 85
4.3.2 Códigos tóricos $[[d^2+1, 2, d]]$ . . . 85

5 Novos Códigos Quânticos Tóricos **87**
5.1 Formas Quadráticas, Reticulados e Poliminós . . . 88
5.1.1 Formas Quadráticas e Reticulados . . . 88
5.1.2 Poliminós . . . 90
5.2 Conjunto dos Representantes dos Poliminós - Uma Abordagem Algébrica . . . 90
5.2.1 Reprodução dos códigos de Bombin e Martin-Delgado . . . 94
5.2.2 Reprodução dos códigos de Kitaev . . . 94
5.2.3 Nova classe de códigos tóricos $[[d^2, 2, d]]$ . . . 94
5.2.4 Outras classes de códigos tóricos . . . 95
5.2.5 Anel de inteiros Gaussianos . . . 96
5.3 Conjunto dos Representantes dos Poliminós - Uma Abordagem Combinatorial . . . 97

6 Códigos TQC em Superfícies Compactas com $g \geq 2$ **101**
6.1 Geometria Hiperbólica 102
6.2 Modelo Planar de uma Superfície 106
6.2.1 Geração de uma superfície a partir de um polígono P' 108
6.2.2 Classificação topológica de superfícies 111
6.2.3 Critério para escolha do polígono P' 112
6.3 Tesselação $\{p,q\}$ 115
6.4 Construção de Códigos Quânticos Topológicos 116
6.4.1 Operadores e parâmetros 117
6.4.2 Distância do código 118
6.4.3 Tabelas de códigos quânticos topológicos 119
6.5 Reprodução de Códigos Conhecidos 124
6.5.1 Código tórico de Kitaev revisitado 124
6.5.2 Classe de códigos com distância 3 em superfícies com gênero $g \geq 2$ 124

Conclusões **129**

Bibliografia **133**

Lista de Figuras

2.1 Sistema de comunicação. 13
2.2 Esferas de Lee de raio $t = 1,2,3$. 22

3.1 Esfera de Bloch. 37

4.1 Reticulado quadrado do toro. 70
4.2 Os ciclos C e C' são homologicamente triviais no reticulado e no reticulado dual, respectivamente. Os demais ciclos são homologicamente não-triviais no reticulado e no reticulado dual. 73
4.3 Movimento de anyons no espaço-tempo. 79
4.4 Cordas e partículas. 80
4.5 Uma partícula tipo-x movendo-se em torno de uma partícula tipo-z. 82
4.6 Geradores de tranças e relações. 83
4.7 Equação de Yang-Baxter. 83
4.8 Código $[[9,1,3]]$ equivalente ao código de Shor. 86
4.9 Reticulados do código de Kitaev e do código de Bombin e Martin-Delgado com $d = 3$. 86

5.1 Reticulado $\mathbb{Z}^2$ gerado por v_1 e v_2. 89
5.2 Duas representações de regiões com área 5. 91
5.3 Código de Kitaev $[[8,2,2]]$. 95
5.4 Duas representações do código $[[16,2,4]]$. 95
5.5 Código $[[6,2,2]]$. 98
5.6 Código $[[14,2,3]]$. 99

6.1 Exemplo de emparelhamento de lados de um octógono hiperbólico cujo ciclo elíptico é $\gamma_4^{-1}\gamma_3^{-1}\gamma_4\gamma_3\gamma_2^{-1}\gamma_1^{-1}\gamma_2\gamma_1$. 109
6.2 Grupo de Klein - um 14-gon com tesselação $\{7,3\}$ dentro. 114
6.3 Transformação de emparelhamento de lados $\gamma(s_i) = s_{i+2g}$. 115
6.4 Comprimento hiperbólico $(2a)$ da menor geodésica ligando lados identificados de P'. 118
6.5 Comprimento da aresta (c) da tesselação $\{p,q\}$. 119

Lista de Tabelas

2.1 Arranjo padrão. 18

3.1 Portas lógicas para dois bits. 45
3.2 Portas quânticas para um qubit. 46
3.3 Porta CNOT. 47
3.4 Síndromes de erros. 51
3.5 Resultados das medidas de Z_1Z_2, Z_2Z_3. 52
3.6 Resultados das medidas de X_1X_2, X_2X_3. 54
3.7 Geradores e operações lógicas do código de Shor. 67
3.8 Geradores e operações lógicas para o código $[[5,1,3]]$. 68

6.1 Polígonos que geram superfícies compactas. 113
6.2 Tesselações e parâmetros dos TQC para $g = 2$ e $d_h = 3.0571$. 121
6.3 Tesselações e parâmetros dos TQC para $g = 3$ e $d_h = 3.9833$. 121
6.4 Tesselações e parâmetros dos TQC para $g = 4$ e $d_h = 4,596$. 122
6.5 Tesselações e parâmetros dos TQC para $g = 5$ e $d_h = 5,0591$. 122
6.6 Códigos com distâncias $d = 3,4$ e 5. 123
6.7 Códigos quânticos topológicos derivados de mergulhos de grafos K_s em superfícies compactas. 126
6.8 Códigos derivados de mergulhos de grafos segundo a sequência a_m. 127
6.9 Códigos derivados de mergulhos de grafos segundo a sequência b_m. 127

Capítulo 1

Introdução

O estudo dos códigos corretores de erros que teve sua origem na teoria da informação introduzida por Shannon em 1948, [68], tem por objetivo transmitir e armazenar dados de maneira confiável, ou seja, de modo que ao recuperar essa informação, seja possível detectar e corrigir erros. Essa teoria está em plena atividade e com várias aplicações em diferentes áreas, sendo uma delas a teoria de códigos quânticos corretores de erros cujo objetivo é proteger a informação quântica de erros, como por exemplo a *decoerência*.

A construção dos códigos quânticos corretores de erros está fortemente baseada nas propriedades de códigos corretores de erros clássicos. Há alguns anos produz-se códigos quânticos cada vez mais eficazes permitindo a evolução do estudo da computação quântica. O primeiro código quântico foi proposto por Shor em 1995, um análogo quântico para o código de repetição clássico, [70]. Independentemente outro código quântico foi proposto por Steane em 1996, [72]. Esses códigos foram depois aprimorados pelos *códigos CSS*, definidos por Calderbank e Shor, [15], e Steane [73]. Ainda em 1996, Gottesman propõe uma classe de códigos mais abrangente chamada *códigos estabilizadores*, [38], da qual os códigos CSS fazem parte. Os códigos estabilizadores baseiam-se em teoria de grupos, um código nesta classe é um subespaço invariante por um subgrupo Abeliano do grupo de Pauli, chamado *subgrupo estabilizador* cujos elementos são operadores unitários chamados *operadores estabilizadores*.

Pode-se, portanto, observar que para o desenvolvimento da teoria de códigos quânticos corretores de erros se faz necessário a compreensão da mecânica quântica, álgebra linear e teoria de grupos. Neste capítulo, inicialmente faremos uma breve revisão de mecânica quântica. Em seguida, introduzimos os pilares da computação quântica e da teoria de codifica-ção quântica, onde ressaltamos uma linha de estudo conhecida como *códigos quânticos topológicos* da qual nossa pesquisa faz parte. Por fim, descrevemos nosso objetivo e como ele será tratado na tese.

1.1 A Nova Teoria Física

É comum considerar-se que a mecânica quântica surgiu em 1900 a partir de um artigo publicado por Max Planck, no qual foi proposto que o processo de produção de luz por um corpo aquecido se dá através de pacotes de energia, chamados *quanta*. Em um dos seus famosos trabalhos em 1905, Einstein usou a idéia de *quanta* introduzida por Planck para mostrar que a luz se propaga na forma de pacotes de energia, ou melhor, a luz é formada de corpúsculos chamados *fótons*. Neste trabalho, Einstein explica o efeito fotoelétrico, o que lhe rende o Prêmio Nobel em 1921. Antes, porém, já era conhecido dos estudos de Thomas Young em 1800, que a luz é um fenômeno ondulatório. Em 1909, Einstein publica um artigo em que mostra que as flutuações de energia de radiação exibiam características de partículas e de onda.

Essas idéias vão de encontro às características determinísticas da física clássica e por isso causam desconforto em muitos pesquisadores, inclusive no próprio Einstein. Alguns anos depois, Louis de Broglie propôs que além da luz, outras partículas elementares da matéria, como elétrons e prótons, também podem se comportar como ondas. Essa teoria ficou conhecida como *dualidade onda-partícula* e é premiada com o Prêmio Nobel em 1929. Com isso, a idéia de que átomos e fótons pudessem ter um caráter ambíguo, de onda e de partícula, ganha ainda mais força.

Em 1907, o físico alemão Werner Heisenberg enunciou o que depois ficaria conhecido como *princípio de incerteza de Heisenberg*: é impossível conhecer com precisão a posição e a velocidade de uma partícula ao mesmo tempo. Ou seja, quanto mais se sabe de uma dessas grandezas, menos se sabe sobre a outra. Isso agrava o desconforto diante da teoria quântica. Outras características quânticas ainda mais estranhas foram observadas no estudo das partículas, como a propriedade de não-localidade, a qual Einstein se referia como uma "ação fantasmagórica à distância".

Assim mesmo a física quântica foi formalizada e até hoje é questionada por alguns pesquisadores. Porém, não há como negar o sucesso dessa teoria em prever o comportamento de sistemas físicos. Muitos nomes, além dos já citados, contribuíram para o surgimento dessa nova teoria: Niels Bohr, Erwin Schrödinger, Max Born, John von Neumann, Paul Dirac, Wolfgang Pauli, Richard Feynman, J. S. Bell, entre outros ilustres.

Um dos principais fenômenos observados na mecânica quântica, e completamente estranho para a mecânica clássica, é que a energia deve ser quantizada. Daí decorre o nome "quantum" que em latim significa quantidade.

Define-se, portanto, como mecânica quântica o estudo dos sistemas físicos nos quais os efeitos quânticos são relevantes. Isso ocorre em dimensões próximas ou abaixo da escala atômica, tais como

moléculas, átomos, elétrons, prótons e outras partículas subatômicas, e também ocorre em situações de escalas macroscópicas, como nos casos da *supercondutividade* e *superfluidez*. Em geral, a escala que regula a manifestação dos efeitos quânticos é conhecida como o *raio de Bohr*. Portanto, a mecânica quântica generaliza a mecânica clássica e fornece descrições exatas para muitos fenômenos anteriormente inexplicados.

Observe que os sistemas físicos não são estacionários, ou seja, cada sistema ocupa um estado em um determinado instante e então evolui para outro estado. As leis da física devem descrever como ocorre essa evolução. No formalismo da mecânica quântica, o estado de um sistema em um dado instante de tempo pode ser representado de duas formas principais: por uma função de onda ou por um vetor num espaço vetorial complexo chamado *vetor estado*. A notação usada em mecânica quântica para representar o vetor estado é chamada *ket*, $|\cdot\rangle$, e foi introduzida por Dirac. Essas representações de estados de um sistema são completas e equivalentes, e as leis da mecânica quântica descrevem como vetores de estado e funções onda evoluem no tempo. Estes objetos matemáticos abstratos permitem o cálculo da probabilidade de se obter resultados específicos em um experimento concreto. Para compreender tais cálculos é necessário o conhecimento de alguns fundamentos de álgebra linear, tais como os conceitos de operador, autovetor e autovalor.

Essencialmente, a mecânica quântica é uma estrutura matemática para o desenvolvimento de uma teoria física. A conexão entre o mundo físico e o formalismo da mecânica quântica é dado pelos *Postulados da Mecânica Quântica*, [56].

Postulado 1

A qualquer sistema físico isolado existe associado um espaço vetorial complexo com produto interno (ou seja, um espaço de Hilbert), conhecido como espaço de estados do sistema. O sistema é completamente descrito pelo seu vetor de estado, um vetor unitário no espaço de estados.

Postulado 2

A evolução de um sistema quântico fechado é descrita por uma transformação unitária. Ou seja, o estado $|\psi\rangle$ de um sistema em um tempo t_1 está relacionado ao estado $|\psi'\rangle$ do sistema em t_2 por um operador unitário U que depende somente de t_1 e t_2:

$$|\psi'\rangle = U|\psi\rangle.$$

Postulado 2'

A evolução temporal do estado de um sistema quântico fechado é descrita pela equação de Schrödin-

ger:

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle.$$

Nessa equação, $\hbar$ é uma constante física chamada constante de Planck, cujo valor é determinado experimentalmente. Na prática, é comum absorver o fator $\hbar$ dentro de H, efetivamente convencionando-se $\hbar = 1$. H é um operador Hermitiano conhecido como Hamiltoniano do sistema.

Postulado 3

As medidas quânticas são descritas por determinados operadores de medida $\{M_m\}$. Esses operadores atuam sobre o espaço de estados do sistema. O índice m se refere aos possíveis resultados da medida.

Postulado 4

O espaço de estados de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas individuais.

O primeiro postulado estabelece a arena na qual se desenvolve a mecânica quântica. O segundo postulado mostra como o estado de um sistema quântico evolui com o tempo, ou seja, mostra qual a relação entre estados em dois instantes de tempo diferentes de um sistema quântico fechado. A dinâmica desse sistema é dada pela equação de Schrödinger, e portanto por transformações unitárias. O postulado 3 explica como extrair informações de sistemas quânticos. Finalmente, o quarto postulado estabelece como espaços de estados de sistemas quânticos diferentes devem ser combinados para formar sistemas compostos.

Foi mencionado que um dos principais aspectos da física quântica é a dualidade onda-partícula. Essa característica de onda foi interpretada por Max Born como uma medida de probabilidade de se encontrar a partícula em uma determinada posição em um determinado tempo. Isso leva a uma propriedade quântica muito peculiar chamada *superposição*.

Uma *superposição de estados* é obtida quando se soma todas as possibilidades de estados para uma determinada partícula. A superposição também é um estado, ou seja, uma partícula que se encontra em um estado de superposição está fazendo tudo o que é possível ela fazer. Classicamente, isso é um absurdo. É como se a partícula pudesse estar simultaneamente em várias posições diferentes.

O sistema fica numa superposição de estados até que uma *observação* ou *medida* seja feita. Ao se fazer uma medida, uma única possibilidade é selecionada e esta será a única ocorrência do sistema. Todas as outras possibilidades que estavam acontecendo no sistema simplesmente desaparecem, ou se anulam, e o estado observado passa a ser o único real. Assim, a superposição é a possibilidade de um

objeto quântico assumir uma combinação de probabilidades que seriam mutuamente excludentes de acordo com a nossa intuição clássica.

Em 1935, Albert Einstein, Boris Podolsky e Nathan Rosen publicaram um artigo onde acreditavam demonstrar que a teoria quântica não era completa, [26]. O argumento usado era que faltava algum "elemento de realidade". Esse elemento usado como critério pelos autores funcionava como uma propriedade que deveria existir independentemente da medida realizada no sistema. Após 30 anos, foi comprovado experimentalmente que essa idéia não era válida. A chave para essa invalidação experimental é conhecida como *desigualdade de Bell*. A conclusão desse fato é que o mundo não é localmente realístico, [56]. Isso leva a outra característica quântica espantosa, a não-localidade. Tal característica possibilita a criação de conjuntos de partículas que apresentam fortes correlações entre suas propriedades. Partículas que apresentam essa propriedade são ditas *emaranhadas*. Ou seja, as propriedades de um estado emaranhado estão armazenadas no estado como um todo, e não em cada partícula individual, não importando a distância entre eles. Consequentemente, qualquer interação com um estado emaranhado, como por exemplo, uma medida, afeta simultaneamente tudo que está emaranhado com ele.

Essa propriedade abre um novo mundo de possibilidades em termos de informação e computação. Uma das principais aplicações do emaranhamento está relacionada à criptografia quântica, que explora a não-localidade quântica para transmitir mensagens com segurança absoluta. Outra aplicação é a possibilidade de transportar a informação quântica de um lugar para outro sem que ocorra o deslocamento através de um meio físico. Esse processo é conhecido como *teletransporte quântico*. Recentemente, em janeiro de 2009, foi publicado um artigo na revista *Science* pelo grupo do Joint Quantum Institute, no qual é descrito o teletransporte de um estado quântico diretamente de um átomo para outro por uma distância significativa, [59]. Esse experimento descreve um teletransporte com 90% de eficiência na recuperação da informação original.

1.1.1 A unidade de informação quântica

A unidade de informação quântica é o *bit quântico*, mais comumente chamado *qubit*. Um qubit pode assumir além dos estados $|0\rangle$ e $|1\rangle$, todos os outros estados correspondentes às combinações lineares desses dois estados. Isso equivale às superposições de $|0\rangle$ e $|1\rangle$.

Podemos escrever um estado de superposição para um qubit na forma

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

onde $\alpha, \beta \in \mathbb{C}$ e a restrição $|\alpha|^2 + |\beta|^2 = 1$ deve ser satisfeita.

Essa superposição de estados significa que o estado $|\psi\rangle$ está simultaneamente nos estados $|0\rangle$ e $|1\rangle$. Após a medida, o estado deve colapsar para $|0\rangle$ ou $|1\rangle$ com suas respectivas probabilidades, $|\alpha|^2$ e $|\beta|^2$.

Pode-se se ter a falsa idéia de que um estado em superposição pode conter uma quantidade infinita de informações, porém ao se medir o qubit o resultado sempre será um estado $|0\rangle$ ou $|1\rangle$. No entanto, pode-se manipular a superposição até que a medida seja feita em um momento mais oportuno, resultando em um melhor aproveitamento dessa propriedade.

No caso geral, o estado $|v\rangle$ com n qubits, é uma superposição dos 2^n estados $|00\ldots0\rangle$, $|00\ldots1\rangle$, $\ldots,|11\ldots1\rangle$, onde a sequência dentro de cada *ket* é a representação binária dos números $0,1,\ldots,2^n-1$, e pode ser escrito como

$$|v\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

com a restrição

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

Os estados $|0\rangle$ e $|1\rangle$ também podem ser representados na forma matricial da seguinte maneira:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Assim, a superposição $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, pode ser escrita na forma

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

A representação matricial é conveniente para compreender as operações que estão sendo realizadas.

1.1.2 Vantagens que a mecânica quântica pode trazer para a computação

A necessidade de uma computação baseada em propriedades quânticas existe por diversas razões. Segundo a lei de Moore, a cada 18 meses a capacidade de processamento dos computadores dobra, enquanto os custos permanecem constantes. De fato, isso vem se confirmando, e atualmente o tamanho dos componentes já se aproxima da escala atômica onde as leis quânticas devem ser respeitadas. Outra razão está relacionada a complexidade computacional. Devido às propriedades quânticas, como superposição e emaranhamento, imagina-se que um computador quântico possa ser mais eficiente do que um computador convencional. Isto é, supõe-se que um computador quântico use menos passos computacionais para a realização de tarefas. Dentro da classificação de complexidade computacional,

a computação quântica encontra-se em uma classe chamada *BQP* (Bound-error, quantum, polynomial time). Essa classe inclui todos os problemas da classe P (Polynomial time) e também alguns outros problemas da classe NP (Nondeterministic polynomial time), como o problema da fatoração de inteiros em componentes primos. Esse problema foi resolvido pelo algoritmo de Shor com ganho exponencial de velocidade, [69]. Sem dúvida um resultado impressionante.

Além do algoritmo de Shor, outro algoritmo quântico que demonstra a eficiência que características quânticas podem proporcionar à computação é o algoritmo de Grover que faz uma busca em uma lista de dados com ganho quadrático de velocidade sobre os algoritmos usados em computação clássica, [43]. Apesar de não ser um resultado tão impressionante em termos de velocidade, é bastante importante devido a sua aplicação em outros problemas. Uma das razões dessa melhora na velocidade se deve a possibilidade de se avaliar paralelamente a mesma função para diversas variáveis.

Outro problema que só poderá ser resolvido em um computador quântico é a simulação de sistemas quânticos. Por esses motivos, não há como negar a necessidade da construção de tais computadores, bem como as pesquisas em computação e informação quântica. Atualmente, existem várias propostas experimentais para a construção de um computador quântico. Porém, esse trabalho é bastante árduo devido às diferenças entre a informação quântica e a informação clássica. Uma dessas dificuldades é a fragilidade da informação quântica. Interações do sistema com o ambiente a sua volta podem destruir os estados de superposição provocando a perda de informação. Esse processo é chamado *decoerência*.

1.2 A Teoria dos Códigos Quânticos Corretores de Erros

A decoerência pode destruir as características quânticas. Esse problema pode ser contornado isolando-se bem o sistema do ambiente que o cerca. Porém, para sistemas maiores, esta tarefa é bastante complicada. Uma maneira de superar essa dificuldade é usando códigos quânticos corretores de erros. Esses códigos funcionam codificando os estados quânticos de forma a torná-los resistentes à ação do ruído, e depois decodificando-os no momento em que se deseja recuperar os estados.

Os códigos quânticos corretores de erros têm sua construção fortemente estruturada nos códigos lineares clássicos. Porém, existem algumas diferenças fundamentais entre informação clássica e informação quântica que devem ser contornadas, tais como a impossibilidade de copiar um qubit arbitrário e o fato de medidas destruirem a informação quântica, impossibilitando sua recuperação.

Dentro da classe de códigos estabilizadores, uma linguagem alternativa, usando topologia, foi introduzida por Kitaev. Sua proposta foi usar certas propriedades de partículas confinadas em um plano para realizar *computação quântica topológica*. Esse nome se deve ao fato de que essas propriedades

estão relacionadas à *topologia* do sistema físico. Assim, deformações contínuas causadas pelo ambiente não seriam capazes de alterar tais propriedades, e então teríamos naturalmente uma computação quântica tolerante à falhas.

Kitaev inicia esse estudo com os *códigos tóricos*, [48]. Para construir esses códigos, qubits são associados às arestas de um reticulado quadrado de um toro. Assim, o número total de arestas fornece o comprimento do código. Os operadores estabilizadores estão relacionados com os vértices e faces desse reticulado, os qubits codificados são dados de acordo com o gênero da superfície, no caso o toro, e a distância do código é determinada pelo grupo de homologia da superfície. Esses códigos podem ser generalizados para uma classe conhecida como *códigos quânticos topológicos*, considerando outras superfícies orientáveis bidimensionais diferentes do toro.

M. Freedman e D. Meyer, em [31], construíram códigos sobre o plano projetivo $\mathbb{R}P^2$, seguindo os mesmos princípios da construção dos códigos tóricos de Kitaev. Além desses trabalhos, outros códigos quânticos topológicos foram apresentados em [13], cujos autores Bombin e Martin-Delgado consideram uma nova visão do código de Kitaev e, a partir disso, propõem uma melhora do comprimento do código tórico além de mostrar uma classe de códigos quânticos com distância 3 resultantes de mergulhos de grafos completos em superfícies com gêneros correspondentes.

1.3 Proposta da tese

A visão dos códigos tóricos lançada por Bombin e Martin-Delgado abre espaço para o estudo dos códigos quânticos tóricos relacionando-os a uma área já conhecida da teoria de codificação clássica, os *códigos reticulados*. A partir dessa conexão é possível obter uma quantidade incontável de novos códigos quânticos tóricos, utilizando ferramentas matemáticas como teoria de grupos e combinatória. Essa é a primeira parte da proposta de estudo desta tese.

Além disso, propomos o estudo e construção de códigos quânticos topológicos em superfícies com gênero $g \geq 2$ de modo similar à construção de Kitaev. Anterior a este trabalho, apenas a classe de códigos descrita por Bombin e Martin-Delgado em [13] apresentava parâmetros de códigos em superfícies com gênero maior que um, apesar de Kitaev em [48] mencionar a possibilidade da existência de tais códigos. Porém, o caminho usado aqui difere do caminho usado por Bombin e Martin-Delgado.

Nossa proposta de construção segue os passos usados na construção de Kitaev, contudo levando em consideração a geometria relacionada às superfícies com gênero $g \geq 2$, a *geometria hiperbólica*. Apesar das diferenças que esta geometria tem da geometria Euclidiana, é possível seguir naturalmente o processo de construção utilizando as propriedades e relações particulares da geometria hiperbólica.

1.4 Descrição da tese

Devido a esse trabalho estar na interface de áreas como engenharia, matemática e física, existe a necessidade de revisão de conceitos e teorias de todas essas áreas. Assim, sua organização é dada da seguinte maneira:

O **Capítulo 2** estabelece o objetivo de estudo dos códigos corretores de erros, e a estrutura matemática dos códigos lineares que formarão a base para a teoria dos códigos quânticos corretores de erros.

No **Capítulo 3**, inicialmente é feita uma ampla revisão da mecânica quântica, suas propriedades e estrutura algébrica. Em seguida, são estabelecidas as distinções entre informação quântica e clássica, e finalmente são apresentados os códigos quânticos corretores de erros, com destaque para os códigos de Shor, os códigos CSS, e os códigos estabilizadores.

O **Capítulo 4** é dedicado à computação quântica topológica e aos códigos quânticos topológicos existentes na literatura. Neste capítulo é apresentada a quasipartícula *anyon* utilizada para a realização desse tipo de computação. Lembramos que, apesar de estarmos trabalhando na interface da física, nosso interesse não é aprofundar conceitos físicos, mas sim deixá-los claros o suficiente para a compreensão deste trabalho.

Apresentamos nossos primeiros resultados no **Capítulo 5** referente à construção de novos códigos quânticos tóricos. Para isso, fazemos uma revisão de reticulados, formas quadráticas e álgebra abstrata.

O **Capítulo 6** apresenta a construção de códigos quânticos topológicos em superfícies compactas com gênero $g \geq 2$. Para essa construção se faz necessária a revisão de geometria hiperbólica, e de conceitos como tesselações hiperbólicas, modelos planares, característica de Euler, entre outros. Este capítulo encerra-se com uma discussão sobre os códigos obtidos, inclusive a reprodução de outros códigos descritos na literatura, e a apresentação em tabelas de tais códigos para superfícies com gênero $g = 2, 3, 4$ e 5.

Finalmente concluímos o trabalho com uma avaliação dos resultados e os possíveis trabalhos decorrentes.

Capítulo 2

Códigos Corretores de Erros Clássicos

Em 1948, o matemático Claude. E. Shannon publicou dois trabalhos que deram origem a teoria da informação. Possivelmente, uma das principais contribuições do trabalho de Shannon foi a definição matemática do conceito de informação. Através dos teoremas de codificação para canais sem ruído e para canais ruidosos, ficam estabelecidas as condições para a transmissão de informação através de um canal de comunicação, [68]. O primeiro desses teoremas quantifica os recursos físicos necessários para armazenar a informação fornecida por uma fonte. Já o segundo, quantifica a informação que pode ser transmitida com confiabilidade através de um canal com ruído. Neste último teorema, Shannon mostra que a probabilidade de erro na decodificação é arbitrariamente pequena se a taxa de transmissão de informação R (expressa em bits por segundo) for menor que a capacidade do canal C (também expressa em bits por segundo).

Apesar do teorema de codificação para canais com ruído garantir a existência de códigos que podem atingir um limitante superior para a proteção contra erros, não fica evidenciado quais os códigos que podem ser utilizados para alcançar esse limitante. A pesquisa em busca de tais códigos deu origem à *teoria dos códigos corretores de erros*.

Neste capítulo é feita uma breve revisão da teoria dos códigos corretores de erros clássicos a fim de facilitar o entendimento da teoria dos códigos quânticos corretores de erros definido no capítulo 3. Para esta revisão foram usadas as referências [11, 44, 50, 51, 52, 61].

2.1 Códigos Corretores de Erros

Os códigos corretores de erros estão presentes em nosso dia-a-dia. Um exemplo muito simples disso é o nosso idioma. Considere o alfabeto A da língua portuguesa composto de 26 letras, espaço em branco, o c cedilha e as vogais acentuadas. Uma palavra da língua portuguesa pode ser considerada

como um elemento do conjunto A^{27}, onde 27 é o comprimento da palavra mais longa desse idioma. Matematicamente, a língua portuguesa pode ser vista como um subconjunto próprio $\mathscr{C}$ de A^{27}. Suponha que, ao escrever uma palavra, produz-se a sequência de letras "cathorro". Como essa palavra não é um elemento de $\mathscr{C}$, percebe-se que houve um erro. Neste caso, a correção é simples, pois no conjunto $\mathscr{C}$, existe uma palavra muito parecida com essa, a saber "cachorro". Porém, se a palavra "pato"for escrita erroneamente como "gato"ou como "rato", não é possível detectar o erro, já que essas três palavras existem no conjunto $\mathscr{C}$. Portanto, do ponto de vista dos processos de codificação e decodificação, esse não é um código muito eficiente, [44].

O processo de transmissão de informação resume-se a informação vinda de uma *fonte* e destinada a um *receptor*, através de um meio conhecido como *canal*. Se o canal não tem ruído, então a informação enviada será recebida sem alteração, porém na prática ruído é adicionado à informação resultando na introdução de erros pelo canal. A finalidade do código é detectar e talvez corrigir esses erros.

Ao utilizar redes sem fio, ao ouvir um CD ou assistir um DVD, ou mesmo quando se fala ao telefone, faz-se uso de códigos corretores de erros. Um código desta classe, basicamente, acrescenta dados adicionais a cada informação que deve ser transmitida ou armazenada, de maneira que ao recuperar essa informação, seja possível detectar e corrigir erros. Por exemplo, considere um tabuleiro de xadrez e a peça que representa o *rei*. O rei se move do centro de uma casa para o centro de outra casa contígua nos sentidos Norte, Sul, Leste e Oeste. As direções nas quais o rei pode se mover são codificadas pelos elementos do conjunto $\{0,1\} \times \{0,1\}$ da seguinte maneira:

$$Norte \to 00 \quad Leste \to 10$$

$$Sul \quad \to 01 \quad Oeste \to 11$$

Essa codificação é chamada *código de fonte*. Suponha que desejamos movimentar o rei através de um controle remoto e que o sinal no caminho sofra interferência. Por exemplo, envia-se a mensagem 01, porém a mensagem recebida é 00. Dessa forma, o rei se desloca para o norte em vez de ir para o sul. Para evitar esse tipo de problema pode se recodificar as palavras de modo a introduzir redundância que permita detectar e corrigir erros. Considere a seguinte recodificação:

$$00 \to 00000 \quad 10 \to 10110$$

$$01 \to 01011 \quad 11 \to 11101$$

Novamente suponha que a direção para a qual o rei deve se deslocar seja o sul, ou seja, a informação enviada é 01011, porém a mensagem recebida é 01111. Neste caso é possível detectar o erro quando

se compara a mensagem recebida com todas as possíveis palavras do código e percebe-se que esta não pertence ao código. Além disso, a palavra do código que tem menor número de componentes diferentes da mensagem recebida é 01011, que é exatamente a mensagem enviada. Portanto, é possível corrigir o erro.

Observe que nesse exemplo, os dois primeiros bits na recodificação, são os bits originais do código de fonte, e os bits restantes são as redundâncias introduzidas. Esse novo código é chamado *código de canal*. Esse procedimento pode ser esquematizado na Figura 2.1 que representa um modelo de um sistema de comunicação típico.

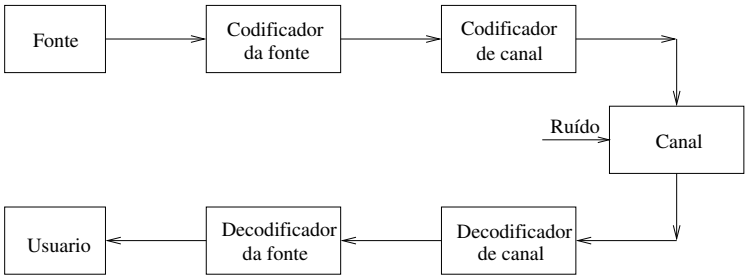

Figura 2.1: Sistema de comunicação.

Nessa linguagem, podemos dizer que os códigos corretores de erros transformam o código de fonte em código de canal, de modo a detectar e corrigir erros na recepção, e decodificam o código de canal em código de fonte.

Matematicamente um código corretor de erros, ou simplesmente CCE, é definido em seguida.

Definição 1 *Considere um conjunto finito K chamado alfabeto. Um código corretor de erros $\mathscr{C}$ é um subconjunto próprio qualquer de K^n, para algum número inteiro n.*

Voltando ao exemplo da língua portuguesa, vimos que não foi possível detectar o erro entre as palavras "pato"e "gato"pois além de serem palavras muito parecidas pertencem ao mesmo conjunto. Intuitivamente, o conceito de distância entre essas palavras é utilizado quando se diz que essas são palavras parecidas. Matematicamente, a definição de distância entre duas palavras **v** e **w** pertencentes a um mesmo código $\mathscr{C}$ é dada pela *distância de Hamming* que é exatamente o número de posições nas quais as duas palavras diferem. Formalmente, a distância de Hamming entre dois elementos $\mathbf{v} = \{v_1, v_2, \ldots, v_n\}, \mathbf{w} = \{w_1, w_2, \ldots, w_n\} \in \mathscr{C}$ é definida como

$$d(\mathbf{v}, \mathbf{w}) = |\{i; v_i \neq w_i, 1 \leq i \leq n\}|,$$

onde $|\{\cdot\}|$ denota a cardinalidade do conjunto $\{\cdot\}$.

Definição 2 *A distância mínima de um código $\mathscr{C}$ é dada por*

$$d = min\{d(\mathbf{v},\mathbf{w}); \mathbf{v},\mathbf{w} \in \mathscr{C}, \mathbf{v} \neq \mathbf{w}\}.$$

Definição 3 *O peso de um vetor arbitrário não-nulo $\mathbf{v} \in K^n$ é a distância de $\mathbf{v}$ ao vetor todo nulo 0, ou seja,*

$$\omega(\mathbf{v}) := min|\{i : v_i \neq 0\}|.$$

Logo, o peso mínimo de um código $\mathscr{C}$ é dado por

$$\omega(\mathscr{C}) := min\{\omega(\mathbf{x}) : \mathbf{x} \in \mathscr{C} \setminus \{0\}\}.$$

A importância da distância mínima na determinação de bons códigos está relacionada à habilidade de correção de erros como pode ser observado no seguinte teorema.

Teorema 1 [44] *Seja $\mathscr{C}$ um código com distância mínima d. Então, $\mathscr{C}$ pode detectar até $d-1$ erros e corrigir até t erros, onde $t = \lfloor \frac{d-1}{2} \rfloor$.*

Decorre que, quanto maior for a distância mínima d do código $\mathscr{C}$, maior será sua capacidade de detecção e correção de erros.

Dentre os códigos corretores de erros destacam-se duas classes, quais sejam, a dos *códigos de bloco* e a dos *códigos em árvore*. Um código de bloco divide a sequência contínua de dígitos de informação na entrada do codificador em blocos de k símbolos e opera nesses blocos independentemente de acordo com o código usado. Cada possível bloco de informação é associado a uma n-upla de símbolos de canal, onde $n > k$. O resultado é transmitido, corrompido pelo ruído, e decodificado independentemente dos outros blocos. Ao passo que um código em árvore opera na sequência de informação sem dividi-la em blocos individuais. O codificador para um código em árvore também recebe blocos de k símbolos de informação e produz uma sequência codificada de blocos de n símbolos. Entretanto, cada bloco codificado não depende somente dos blocos de mensagens de k símbolos correspondentes na unidade de tempo atual. Também vai depender de m blocos de mensagens anteriores. Portanto, ao contrário dos códigos de bloco, o codificador de um código em árvore tem uma memória m.

O nome "código em árvore" deve-se ao fato que as regras de codificação para esse tipo de código são melhor descritas através de um grafo em árvore. Uma importante subclasse desses códigos é a classe dos códigos convolucionais que são mais simples de implementar que outros tipos de códigos em árvore, [61].

Entre as duas classes de CCE, a classe dos códigos de bloco têm uma teoria mais desenvolvida devido ao fato de estar relacionada à estruturas matemáticas relativamente bem-entendidas. Quanto a capacidade de correção de erros, os códigos de bloco e os códigos convolucionais são similares e possuem as mesmas limitações fundamentais, [61]. Em particular, o teorema de Shannon para canal discreto com ruído é satisfeito para ambos os tipos de códigos.

Como a construção dos códigos propostos neste trabalho baseia-se na teoria clássica de códigos de bloco, não será aprofundada a revisão de códigos em árvore.

2.2 Códigos de Bloco

Como mencionado anteriormente, os códigos de bloco são caracterizados por serem códigos sem memória. Considere um alfabeto K com q símbolos. Identificamos esse alfabeto com os elementos do corpo $\mathbb{F}_q$. O codificador para um código de bloco divide a sequência de informação em blocos de k símbolos, onde cada um desses blocos é representado por uma k-upla $\mathbf{u} = (u_1, \ldots, u_k)$ chamada *mensagem*. No total, existem q^k mensagens diferentes. Após a divisão da sequência de informação, o codificador transforma cada mensagem $\mathbf{u}$ em uma n-upla $\mathbf{v} = (v_1, \ldots, v_n)$ de símbolos discretos chamada *palavra-código*. Se cada uma das q^k mensagens distintas é transformada em uma palavra-código, então existem também q^k palavras-código diferentes. Esse conjunto formado por q^k palavras-código de comprimento n é chamado *código de bloco* com parâmetros (n,k). Algumas vezes a notação usada para o código é (n,k,d), onde d é a distância mínima do código.

Em geral, q é uma potência de um primo p, e o caso mais comum em códigos é quando $q = 2$, conhecido como *binário*. Neste caso, $\mathbb{F}_2 = \{0,1\}$, e os elementos 0 e 1 são chamados *bits*.

A *taxa do código* é dada pela razão $R = \frac{k}{n}$, e pode ser interpretada como o número de símbolos de informação entrando no codificador pelo número de símbolos transmitidos. Nesse processo, cada palavra-código depende unicamente da mensagem de entrada correspondente, e por isso dizemos que o codificador é sem memória.

Para um código ter uma palavra-código distinta associada a cada mensagem enviada, é preciso que $k < n$ ou $R \leq 1$. No caso de $k < n$, os $n-k$ símbolos restantes são os símbolos de redundância. Para uma razão R constante, mais símbolos podem ser adicionados aumentando o comprimento n do bloco. O grande desafio é escolher os símbolos de redundância que permitam uma transmissão confiável através de um canal com ruído.

Em geral, bons códigos são longos e por isso torna-se impraticável descrevê-los através de listas de palavras-código. Para contornar esse problema, o caminho usual é associar aos códigos estruturas

matemáticas que facilitem a execução das operações de codificação e decodificação. Neste sentido, a principal classe dos códigos de bloco é a dos *códigos lineares*.

2.2.1 Códigos lineares

Considere um código de bloco com q^k palavras-código e comprimento n. Se k e n são relativamente grandes, então teremos dificuldade quanto ao espaço para armazenar essas palavras-código. Nesse sentido, códigos de bloco com uma estrutura linear são mais práticos e reduzem a complexidade do codificador.

Definição 4 *Um código de bloco de comprimento n com q^k palavras-código é um código linear (n,k) se suas q^k palavras-código formam um subespaço de dimensão k do espaço vetorial de todas as n-uplas sobre o corpo $\mathbb{F}_q$.*

Observe que um código linear pode ser visto como um subgrupo do grupo aditivo $(\mathbb{F}_q^n,+)$, por esse motivo os códigos lineares são também conhecidos como *códigos de grupo*.

A estrutura linear nos permite fazer algumas observações que serão muito úteis. Uma dessas, é que a distância mínima d entre palavras-código distintas é igual ao peso mínimo de todas as palavras-código não nulas de $\mathscr{C}$, isto é, $d = \omega(\mathscr{C})$.

Outra vantagem de trabalhar com códigos lineares é que como $\mathscr{C}$ é um subespaço vetorial de dimensão k, podemos exibir uma base $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ para $\mathscr{C}$. Assim, qualquer palavra-código $\mathbf{v} = (a_1, a_2, \ldots, a_k) \in \mathscr{C}$ pode ser escrita como combinação linear dos vetores da base, ou seja,

$$\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_k\mathbf{v}_k,$$

onde $a_i \in \{0,1,2,\ldots,q-1\}$ e a soma é realizada módulo q.

Qualquer conjunto de vetores formando uma base para o subespaço $\mathscr{C}$ pode ser usado como as linhas de uma matriz G, chamada *matriz geradora* do código. O espaço das linhas de G é o código linear $\mathscr{C}$, e qualquer palavra-código é uma combinação linear das linhas de G. Se a dimensão do espaço vetorial $\mathscr{C}$ é k, então o número de linhas de G é igual a k, pois as linhas de G são linearmente independentes, ou seja, o posto de G é k. Assim G é uma matriz $k \times n$.

Se $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ é uma base ordenada de um código $\mathscr{C}$, então a matriz geradora G de $\mathscr{C}$ associada a B, cujas linhas são os vetores $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$, é dada por

$$G = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \cdots & v_{kn} \end{pmatrix}.$$

Qualquer correspondência um-a-um entre as k-uplas e as palavras-código pode ser usada como um procedimento de codificação, porém a mais natural é

$$\mathbf{v} = \mathbf{u} \cdot G, \tag{2.1}$$

onde $\mathbf{u}$ é uma k-upla de símbolos de informação a serem codificadas e a n-upla $\mathbf{v}$ é a palavra-código correspondente.

Como essa matriz depende da escolha da base, então ela não é univocamente determinada por $\mathscr{C}$. Entretanto, duas matrizes geradas por um mesmo código podem ser obtidas uma da outra por meio de uma sequência de operações, tais como: permutação de duas linhas, multiplicação de uma linha por um escalar não nulo e adição de um múltiplo escalar de uma linha a outra. Assim, toda matriz geradora G é equivalente a uma matriz na forma escalonada das linhas, e portanto, equivalente a uma matriz da forma $G = (I_k \mid P)$ chamada *matriz de forma sistemática* da matriz geradora, onde I_k é a matriz identidade de ordem k e P é uma matriz $k \times (n-k)$.

Existe uma descrição alternativa de códigos também através de matrizes. Novamente, considere $\mathscr{C}$ um subespaço de dimensão k, seu complemento ortogonal $\mathscr{C}^{\perp}$ formado por todos os vetores ortogonais a $\mathscr{C}$, é um espaço vetorial de dimensão $n-k$, e portanto pode ser usado como um código linear. Uma matriz H de posto $n-k$ cujo espaço linha é $\mathscr{C}^{\perp}$ pode ser considerada uma matriz geradora para $\mathscr{C}^{\perp}$. Então uma n-upla $\mathbf{v}$ é uma palavra-código de $\mathscr{C}$ se, e somente se, ela for ortogonal a todo vetor linha de H, isto é,

$$\mathbf{v}H^T = 0. \tag{2.2}$$

Se $\mathscr{C}$ é um código (n,k), então $\mathscr{C}^{\perp}$ é um código $(n-k,k)$. $\mathscr{C}$ e $\mathscr{C}^{\perp}$ são chamados *códigos duais*. Assim, se um código é o espaço linha de uma matriz, seu dual é o espaço ortogonal, e vice-versa. Dizemos que um código $\mathscr{C}$ é *auto-dual* se $\mathscr{C}$ contém seu dual.

A matriz geradora do código dual H de ordem $(n-k) \times n$, é chamada *matriz verificação de paridade* do código $\mathscr{C}$.

Note que a equação (2.2) é satisfeita para todo $\mathbf{v} \in \mathscr{C}$, em particular, é satisfeita para os k vetores da base da matriz G. Essas k equações podem ser expressas como

$$G \cdot H^t = 0.$$

Computacionalmente é menos complexo verificar se uma palavra-código $\mathbf{v}$ pertence a um código $\mathscr{C}$ através da equação (2.2) do que mostrar que o sistema de n equações com k incógnitas dado pela equação (2.1) admite solução.

Existe uma maneira simples de achar uma matriz verificação de paridade para um código se uma matriz geradora é dada na forma sistemática. Se $\mathscr{C}$ é o espaço linha da matriz $G = (I_k \mid P)$, então $\mathscr{C}$ é o espaço ortogonal de $H = (-P^T \mid I_{n-k})$, onde I_{n-k} é a matriz identidade de ordem $n-k$ e P^T é a matriz transposta de P.

Definição 5 *Dado um código $\mathscr{C}$ com matriz verificação de paridade H, a síndrome de um vetor $\mathbf{v} \in \mathbb{F}_q^n$ é o vetor $H\mathbf{v}^t$.*

A síndrome é um argumento usado para fazer a correção de erros em códigos lineares.

A expressão *padrão de erro* denomina a diferença entre a palavra-código recebida e a palavra-código enviada. Em um código linear $\mathscr{C}$ com parâmetros (n,k), considere um padrão de erro $\mathbf{e} \in \mathbb{F}_q^n$. Como $\mathscr{C}$ é um subgrupo, então $\mathbf{e}+\mathscr{C} = \{\mathbf{e}+\mathbf{v} \mid \mathbf{v} \in \mathscr{C}\}$ é uma classe lateral de $\mathbb{F}_q^n$.

Estabeleça uma tabela da seguinte maneira:

- a primeira linha da tabela deve conter todas as palavras-código de $\mathscr{C}$, começando com a palavra toda nula.
- Das n-uplas de $\mathbb{F}_q^n$ que não foram usadas, escolha aquela com menor peso e chame-a de $\mathbf{e}_1$. A segunda linha da tabela será composta pela classe lateral $\mathbf{e}_1+\mathscr{C}$.
- A j-ésima linha da tabela é formada pela classe $\mathbf{e}_j+\mathscr{C}$, onde $\mathbf{e}_j$ é sempre escolhido como a n-upla em $\mathbb{F}_q^n$ de menor peso que ainda não foi usada.
- Esse procedimento termina quando todas as palavras de $\mathbb{F}_q^n$ tenham sido usadas.

A Tabela 2.1 determinada assim é chamada *arranjo padrão*.

$\mathbf{v}_1 = 0$	$\mathbf{v}_2$	$\mathbf{v}_3$	$\cdots$	$\mathbf{v}_q^k$
$\mathbf{e}_1$	$\mathbf{e}_1+\mathbf{v}_2$	$\mathbf{e}_1+\mathbf{v}_3$	$\cdots$	$\mathbf{e}_1+\mathbf{v}_q^k$
$\mathbf{e}_2$	$\mathbf{2}+\mathbf{v}_2$	$\mathbf{e}_2+\mathbf{v}_3$	$\cdots$	$\mathbf{e}_2+\mathbf{v}_q^k$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
$\mathbf{e}_{q^{n-k}}$	$\mathbf{e}_{q^{n-k}}+\mathbf{v}_2$	$\mathbf{e}_{q^{n-k}}+\mathbf{v}_3$	$\cdots$	$\mathbf{e}_{q^{n-k}}+\mathbf{v}_{q^k}$

Tabela 2.1: Arranjo padrão.

Algumas observações importantes devem ser feitas sobre o arranjo padrão. Cada palavra aparece uma única vez na tabela. Duas palavras estão na mesma classe lateral se, e somente se, possuem a mesma síndrome. A primeira coluna da tabela é formada pelas palavras de peso mínimo dentro de cada classe, e são denominadas os *líderes* das classes laterais.

Uma regra de decodificação por *máxima verossimilhança* para um código linear é completamente descrita pelo arranjo padrão. O receptor utiliza o arranjo padrão para decodificar uma palavra recebida da seguinte maneira:

- recebido **v**, calcule sua síndrome;
- ache o padrão de erro **e** correspondente a essa síndrome na tabela;
- $\mathbf{v} - \mathbf{e}$ é a palavra-código.

Para um código (n,k) sobre $\mathbb{F}_q^n$ uma lista completa consiste de q^n palavras ao passo que a lista dada no arranjo padrão tem apenas q^{n-k} palavras e suas síndromes. Mesmo assim, na prática bons códigos são longos e fazer o arranjo padrão ainda é impraticável para alguns casos.

2.2.2 Parâmetros de qualidade de um código

Existem muitos critérios para determinar a qualidade de um código. Entre esses critérios destacamos o *limitante de Singleton* e o *limitante de Hamming*.

O peso mínimo de um código está relacionado à matriz verificação de paridade segundo o teorema abaixo.

Teorema 2 [44] *Seja H a matriz verificação de paridade de um código $\mathscr{C}$. O peso mínimo de $\mathscr{C}$ é igual a ω se, e somente se, quaisquer $\omega - 1$ colunas de H são linearmente independentes e existem ω colunas de H linearmente dependentes.*

Seja $\mathscr{C}$ um código linear com parâmetros (n,k). Usando a matriz na forma sistemática, decorre do teorema 2 a desigualdade

$$d \leq n - k + 1 \tag{2.3}$$

conhecida como *limitante de Singleton*.

Definição 6 *Um código que satisfaz com igualdade o limitante de Singleton é chamado MDS (*Maximum Distance Separable*).*

Se $\mathscr{C}$ é um código MDS, então seu código dual $\mathscr{C}^{\perp}$ é também MDS.

Em seguida são definidos *códigos perfeitos* e *códigos quasi-perfeitos*.

Definição 7 *Um código é perfeito se os líderes das classes laterais em seu arranjo padrão correspondem a todos os padrões de erro de peso menor ou igual a t, onde $t = \lfloor \frac{d-1}{2} \rfloor$.*

Definição 8 *Se os líderes das classes laterais de um arranjo padrão de um código $\mathscr{C}$ correspondem a todos os padrões de erro de peso menor ou igual a t, alguns de peso $t+1$ e nenhum com peso maior que $t+1$, então esse código é um código quasi-perfeito.*

Um código perfeito corretor de t erros pode corrigir todos os erros de peso menor ou igual a t e nenhum de peso maior que t. Enquanto um código corretor de t erros quasi-perfeito pode corrigir todos os erros de peso menor ou igual a t, alguns erros de peso $t+1$ e nenhum de peso maior que $t+1$. Portanto, um código quasi-perfeito corrige mais erros do que um código perfeito.

Se imaginarmos uma esfera pequena em torno de cada uma das palavras-código de um código, sendo cada esfera de mesmo raio, onde o raio é um número inteiro, então dizer que um código é perfeito é equivalente a dizer que as esferas de raio t em volta das palavras-código são disjuntas, e que juntas contém todos os vetores de comprimento n. Similarmente, um código quasi-perfeito é equivalente a dizer que as esferas de raio $t+1$ em volta das palavras-código podem se sobrepor, e juntas contém todos os vetores de comprimento n.

Seja $\mathscr{C}$ um código linear de comprimento n contendo $M = q^k$ palavras-código e que corrige t erros. Então, as esferas de raio t em volta das palavras-código são disjuntas. Cada uma dessas M esferas contém $1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t$ vetores. Por outro lado, o número total de vetores no espaço das n-uplas é q^n. Logo, fica estabelecido o *limitante de Hamming* ou *limitante de empacotamento por esferas*.

Teorema 3 [52] *Um código corretor de t erros de comprimento n contendo M palavras-código deve satisfazer*

$$M\left[1+\binom{n}{1}(q-1)+\binom{n}{2}(q-1)^2+\ldots+\binom{n}{t}(q-1)^t\right] \leq q^n.$$

Um código perfeito satisfaz o limitante de Hamming com a igualdade.

Tanto os códigos perfeitos quanto os quasi-perfeitos são raros, sendo este último encontrado com mais freqüência.

Um código de grupo binário é chamado *ótimo* se sua probabilidade de erro é a menor possível entre todos os códigos de grupos binários com os mesmos parâmetros n e k. Uma consequência disso é que todo código quasi-perfeito (quando existe para dados n e k) se constitui em um código ótimo.

Outro parâmetro que demonstra a qualidade de um código é a sua taxa de informação R. Quanto mais próxima de 1 melhor. Além disso, já foi mencionado que quanto maior a distância mínima do código, melhor é a capacidade de correção dele.

2.2.3 Exemplos de códigos de bloco

Destacamos alguns exemplos de códigos de bloco que serão usados posteriormente para a definição de códigos quânticos.

Exemplo 2.1 *Código de Repetição de 3 bits*

Um código de repetição é um código simples para proteção de bit contra erros que possam ser introduzidos no canal. A idéia é fazer cópias do bit de informação da seguinte forma:

$$0 \rightarrow 000$$

$$1 \rightarrow 111.$$

Admitindo que o receptor saiba que o processo de codificação usado foi o de repetição, de posse dos três bits recebidos ele deverá decidir qual bit foi enviado originalmente. Por exemplo, suponhamos que um bit foi codificado e enviado de acordo com a exemplificação acima, e que o receptor tenha recebido"101". Então, ele entenderá que o segundo bit foi trocado, e decidirá que o bit enviado foi "1". Porém, se dois bits forem trocados, ele provavelmente irá decidir pelo bit de informação errado.

Em um canal BSC (canal simétrico binário), a probabilidade de inverter o bit transmitido é $p > 0$. Ou seja, o bit será transmitido sem erro com probabilidade igual a $1-p$. Usando o código de repetição de três bits, a probabilidade de erro passa de p para $p_e = 3p^2 - 2p^3$, se $p < \frac{1}{2}$. Logo a codificação torna a transmissão mais confiável.

Neste exemplo, um bit de fonte foi codificado em um símbolo de canal de três bits. Ou seja, a taxa desse código é $\frac{1}{3}$.

O código de repetição tem uma ótima capacidade de correção de erro, porém transmite apenas um digito de mensagem por bloco, ou seja, a taxa de informação é baixa.

Exemplo 2.2 *Código de Hamming*

O código de Hamming corrige um erro e é importante devido a facilidade de codificação e decodificação Além disso, este é um código perfeito. Vejamos o caso binário.

Para que um código linear binário seja capaz de corrigir todos os padrões de erro de um único erro de canal, as colunas de sua matriz verificação de paridade H devem ser distintas e não-nulas. De fato, se houver uma coluna toda nula, um erro nessa posição não afetará a síndrome e portanto, não será detectável. Por outro lado, se houver duas colunas iguais, então erros nessas posições serão indistinguíveis. Assim, se H tem m linhas, então existem somente $2^m - 1$ colunas livres, a saber os

representantes binários de $1,2,\ldots,2^m-1$. *Logo, um código binário de Hamming* $\mathbf{H}_m$ *de comprimento* 2^m-1, *para* $m \geq 2$, *tem como matriz verificação de paridade H a matriz cujas colunas consistem de todos os vetores binários não-nulos de comprimento m, cada um aparecendo uma única vez e em qualquer ordem. Portanto,* $\mathbf{H}_m$ *é um código* $(2^m-1, 2^m-1-m, 3)$.

Por exemplo, considere um código de Hamming com $m = 3$, *então seus parâmetros são* $(7,4,3)$ *e a matriz verificação de paridade desse código é dada por*

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Ou ainda, na forma sistemática

$$H' = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Observe que os códigos de bloco e convolucional conhecidos são baseados no conceito de distância de Hamming. Entretanto, a *distância de Lee*, embora não seja amplamente usada, é mais natural para certos tipos de canais.

O *peso de Lee* de uma n-upla $(a_{n-1},\ldots,a_1,a_0)$, a_i escolhido no conjunto $\{0,1,\ldots,q-1\}$, onde q é um inteiro positivo arbitrário, é definido como

$$\omega_L = \sum_{i=0}^{n-1} |a_i|,$$

onde $|a_i| = a_i$, se $0 \leq a_i \leq \frac{q}{2}$ ou $|a_i| = q - a_i$, se $\frac{q}{2} \leq a_i \leq q-1$. A *distância de Lee* entre duas n-uplas é portanto, definida como o peso de Lee de sua diferença, [61].

Para $q = 2$ e $q = 3$ as distâncias de Lee e Hamming coincidem, enquanto que para $q > 3$, a distância de Lee entre duas n-uplas é maior ou igual a distância de Hamming entre elas.

Exemplo 2.3 *Códigos reticulados são um exemplo de códigos de bloco. Em [36] é mostrado que códigos close-packed ou códigos perfeitos podem ser obtidos através de uma tesselação em um reticulado do toro por translações de esferas de Lee de raio t.*

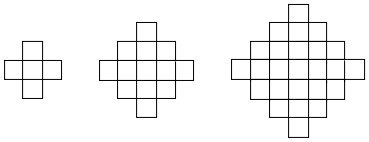

Figura 2.2: Esferas de Lee de raio $t = 1,2,3$.

É possível mostrar que para todo inteiro positivo t dado, existe um código corretor de t erros perfeito, na métrica de Lee, cujo comprimento da palavra-código é $n = 2$*, sobre o alfabeto de inteiros módulo* $q = 2t^2 + 2t + 1$*, [11].*

Capítulo 3

Códigos Quânticos Corretores de Erros

Este capítulo tem por objetivo fazer uma apresentação geral da teoria dos códigos corretores de erros quânticos. Antes, porém, é necessário ter um entendimento dos conceitos centrais da computação quântica e de como se deu seu desenvolvimento. Começamos com um apanhado histórico da evolução da computação quântica na Seção 3.1. Na Seção 3.2 revisamos os principais conceitos e propriedades da mecânica quântica que são importantes para a computação quântica. Na Seção 3.3 apresentamos a estrutura algébrica da computação quântica. A Seção 3.4 é dedicada a teoria dos códigos quânticos corretores de erros, além disso apresentamos os principais códigos que deram origem a essa área de pesquisa. E finalmente na Seção 3.5 detalhamos a classe dos códigos estabilizadores, da qual a nossa proposta é um caso particular.

3.1 Panorama Histórico

A *física quântica* ou *mecânica quântica* surgiu na primeira metade do século XX em meio a uma crise na física. As teorias físicas conhecidas até então, não conseguiam explicar vários resultados de experimentos envolvendo átomos, e à medida que os estudos sobre átomos se aprofundavam mais ineficiente elas se tornavam.

Apesar da mecânica quântica parecer estranha por não concordar com a nossa intuição, essa teoria tem mostrado enorme sucesso em prever o comportamento observado dos sistemas físicos. Os cálculos e os experimentos comprovam a precisão dessa teoria que é aplicada desde os estudos sobre o interior do Sol, passando pela estrutura de átomos, fusão nuclear nas estrelas, supercondutores, estrutura do DNA, até as partículas elementares da Natureza, [56].

A computação quântica baseia-se em propriedades quânticas, porém segue o mesmo caminho anteriormente trilhado pela computação que conhecemos hoje. A *computação clássica*, como ficou co-

nhecida agora, teve suas bases teóricas estabelecidas em 1936 por Alan Turing quando este descreveu matematicamente a noção abstrata do computador programável. Esse modelo ficou conhecido como *máquina de Turing*, e sua propriedade fundamental é que qualquer problema computacional solúvel por qualquer outro computador pode ser resolvido em uma máquina de Turing. Ou seja, se um algoritmo pode ser realizado em algum tipo de computador, então existirá um algoritmo equivalente para uma máquina de Turing universal que realiza exatamente a mesma tarefa. Essa afirmação é conhecida como *tese de Church-Turing*.

Depois do artigo de Turing surgiram os primeiros computadores construídos a partir de componentes eletrônicos. O crescimento dessa área se deu de maneira extraordinária graças a tecnologia de miniaturização dos transistores. Em 1965, Gordon Moore estabeleceu uma lei que ficou conhecida como *Lei de Moore* que diz que a cada 18 meses a capacidade de processamento dos computadores dobra, enquanto os custos permanecem constantes. Essa lei tem se confirmado até hoje, porém existem limites físicos para a redução do tamanho dos componentes. Acredita-se que por volta de 2020 o limite de miniaturização dos transistores terá sido alcançado, já que tais transistores não podem ser menores do que um átomo. Na verdade, a tecnologia atual utilizada na fabricação de computadores já encontra problemas devido ao tamanho dos componentes, pois na escala atômica os efeitos quânticos passam a interferir no funcionamento desses. Esse é um dos motivos para se pensar em uma computação baseada em características quânticas.

Outra justificativa para estudar a computação quântica é que devido às propriedades quânticas imagina-se que um computador quântico possa ser mais *eficiente* do que um computador convencional. Essa noção de eficiência está relacionada a *complexidade computacional*, ou seja, o número de passos computacionais básicos necessários para resolver um dado problema. Essa área de pesquisa tenta estimar como o número de passos computacionais depende do tipo e do tamanho do problema.

Quando um algoritmo para resolver um certo problema utiliza uma quantidade de passos que cresce em tempo polinomial em relação ao tamanho do problema, dizemos que este problema tem uma solução eficiente. Por exemplo, para multiplicarmos dois números de n dígitos cada, usando o algoritmo da multiplicação, precisamos de aproximadamente n^2 operações simples. Por outro lado, para fatorar um número em seus componentes primos, os métodos mais avançados conhecidos em máquina de Turing gastam um tempo que aumenta exponencialmente com o número de dígitos. Para esses casos, onde o crescimento da complexidade computacional é exponencial, dizemos que o problema não tem uma solução eficiente. A mecânica quântica tem propriedades que podem vir em auxílio a essa dificuldade, como a *superposição* de estados que veremos na subseção 3.2.1.

Os problemas que os computadores clássicos podem resolver em tempo polinomial formam a

classe P (Polynomial time) de complexidade. Por exemplo, o problema de ir de uma cidade para a outra a partir de um certo mapa rodoviário com n cidades. Para um valor de n grande, o número de passos computacionais necessários para resolver o problema aumenta com n^2. Outra classe de problemas é conhecida como NP (Nondeterministic polynomial time), e é formada pelos problemas cujas soluções são facilmente verificadas, ou seja, uma vez encontrada uma solução, ela pode ser reconhecida como correta no tempo polinomial, mesmo que seja difícil encontrar tal solução. A classe P está contida na classe NP, e esta última contém um grande número de problemas de interesse prático. Por exemplo, a fatoração de um número de n dígitos em seus fatores primos. Se tivermos a solução, será fácil verificar se ela é de fato a resposta em tempo polinomial, bastando para isso multiplicar os fatores primos. Por outro lado, já foi mencionado que encontrar essa resposta requer uma complexidade de ordem exponencial. O problema de fatoração se encontra na classe NP, e acredita-se que ele não pertença a classe P, pois não se conhece nenhum algoritmo em computação clássica que seja capaz de resolvê-lo em tempo polinomial. Os problemas NP mais difíceis formam outra classe chamada NP completo. Por exemplo, o problema de colorir todos os países de um dado mapa, usando apenas três cores, sem que países vizinhos sejam da mesma cor. Se for encontrado um algoritmo eficiente para qualquer um dos problemas dessa classe, então o algoritmo pode ser adaptado para resolver também todos os outros problemas NP. Dispor de tal algoritmo significa que a classe P seria igual à classe NP. Essa é uma discussão que divide muitos especialistas em computação.

A computação quântica se encaixa nesse panorama da complexidade em uma classe chamada BQP (Bound-error, quantum, polynomial time). Essa classe é formada pelos problemas que podem ser resolvidos eficientemente por computadores quânticos, isso inclui todos o problemas P e também alguns outros problemas NP, como o da fatoração e o problema do logaritmo discreto. No entanto, outros problemas NP e todos os NP completos estão fora da classe BQP, ou seja, um computador quântico não seria capaz de solucioná-los em tempo polinomial. Por outro lado, a classe BQP pode ir além da NP, o que significa que os computadores quânticos podem resolver certos problemas mais rapidamente que os computadores clássicos e ainda verificar a resposta. Além dessas classes, existe também a classe PSPACE formada pelos problemas que um computador convencional pode resolver, porém utilizando um número exponencial de passos. Note que, as classes NP e BQP estão contidas na classe PSPACE. Por esses, e outros motivos que veremos adiante, a computação quântica parece ser tão promissora.

Depois de observar que computadores clássicos tinham grandes dificuldades para simular sistemas quânticos, mesmo os mais simples, o físico Richard Feynman, em 1982, propôs pela primeira vez a idéia de um computador baseado nos princípios da mecânica quântica, [28]. No entanto, a atual

concepção de um computador quântico deve-se ao físico David Deutsch, [23]. Ao tentar consolidar a tese de Church-Turing quanto às teorias físicas, ele percebeu que o aparato computacional a ser usado deveria se basear nos princípios da mecânica quântica. A conjectura de Deutsch, de que um computador universal é suficiente para simular eficientemente um sistema físico arbitrário, ainda não foi provada, nem refutada.

Após Deutsch descrever um computador quântico, houve muitos avanços na pesquisa sobre a capacidade desses computadores. Alguns resultados mostraram uma discreta vantagem desses sobre os computadores clássicos, porém um resultado obtido pelo matemático Peter Shor em 1994 deu força a idéia de que computadores quânticos seriam de fato mais eficientes do que os computadores clássicos. O algoritmo de Shor é o mais famoso e promissor resultado em termos da velocidade de um computador quântico, isso porque ele resolve um problema prático muito mais rapidamente do que os algoritmos conhecidos até então. Shor mostrou que usando características quânticas, um computador quântico seria capaz de fatorar um número com n dígitos com uma quantidade de passos computacionais que cresce polinomialmente em n, [69]. Como já foi mencionado, em computadores convencionais, os melhores algoritmos conhecidos exigem recursos que crescem exponencialmente.

O problema da fatoração de inteiros em componentes primos é famoso no mundo matemático, e tem sua principal aplicação prática em criptografia, como por exemplo, em esquemas de codificação de dados usados por bancos ou em páginas da internet. Isso explica o impacto do trabalho de Shor. Devido ao enorme sucesso desse algoritmo, muitos pesquisadores entraram na busca por outros algoritmos quânticos eficientes. A principal descoberta depois do algoritmo de Shor foi feita em 1996 pelo matemático Lov Grover. O algoritmo proposto por Grover faz uma busca numa base de dados, encontrando ítens específicos que tenham propriedades pré-determinadas, [43]. No caso clássico, para encontrar um item em uma lista de N ítens, onde N cresce exponencialmente à medida que o tamanho do problema aumenta, são necessárias cerca de N operações. O algoritmo de Grover, usando propriedades quânticas, resolve esse mesmo problema com apenas $\sqrt{N}$ operações, o que representa um número muito menor de passos. Apesar de oferecer somente um ganho quadrático de velocidade, esse é um avanço significativo, especialmente por se tratar de um algoritmo bastante usado em outros problemas. Uma característica de muitos algoritmos quânticos e que pode ser observada nos algoritmos de Shor e Grover, é a possibilidade de avaliar funções $f(x)$ para diferentes valores de x simultaneamente, tal particularidade é conhecida como *paralelismo quântico*.

Ao longo da última década pesquisadores mostraram que algoritmos semelhantes e mais modestos, são o limite para muitos outros problemas, [67]. A pesquisa sobre novos algoritmos quânticos continua, no entanto não é apenas nessa linha que se desenvolve a pesquisa em computação quântica.

Em 1984, os físicos Charles Bennett e Gilles Brassard desenvolveram o primeiro protocolo de criptografia quântica, possibilitando trocas de mensagens com segurança absoluta, [9]. O esquema envolve a troca de partículas quânticas de luz (fótons). Na década de 1990, a propriedade quântica conhecida como *emaranhamento* foi bastante investigada no sentido de ser utilizada para solucionar problemas de processamento de informação. Seguiu-se uma quantidade enorme de trabalhos publicados nesse tema. Em 1991, Artur Ekert demonstrou como utilizar o emaranhamento para distribuir chaves criptográficas imunes à espionagem, [27]. Em 1992, Charles Bennett e Stephen Wiesner mostraram como transmitir dois bits clássicos de informação, transmitindo somente um bit quântico, um resultado conhecido como *codificação superdensa*, [10]. Em 1993 uma equipe internacional formada por seis colaboradores explicou como é possível deslocar estados quânticos de um lugar para outro, mesmo quando não existe um canal de comunicação, usando o emaranhamento, em um processo conhecido como *teletransporte quântico*, [55]. E muitas outras aplicações estão sendo estudadas.

Por outro lado, em 1995 Benjamin Schumacher enunciou um análogo quântico do teorema da codificação para canais sem ruído de Shannon, [66], e pôde definir o "bit quântico" como um recurso físico tangível, dando origem à *teoria da informação quântica*. A importância dessa nova área atraiu investimentos de governos e também da indústria. Hoje a teoria quântica de correção de erros está bastante desenvolvida, e permite que um dia os computadores quânticos operem efetivamente na presença de ruído, além de permitir também a comunicação de canais quânticos ruidosos de forma confiável.

A grande dificuldade de efetuar uma computação quântica está envolvida com uma propriedade quântica da superposição. A grosso modo, a superposição de estados permite que um objeto quântico assuma várias posições ao mesmo tempo até ser feita uma *observação* ou *medida*. Imediatamente após a medida, uma única posição é selecionada e o objeto passa a se comportar como um objeto clássico. Enquanto o objeto está em um estado de superposição é possível manipular esse estado e obter vantagens computacionais, porém basta uma simples observação e essa informação colapsa para uma única posição, consequentemente perdendo a superposição. Isso torna a informação quântica bastante vulnerável.

Esse processo de desaparecimento das superposições é chamado *descoerência* ou *decoerência*. A decoerência é o fenômeno de decaimento de estados em superposições e se deve a interação entre os sistemas e o ambiente que o cerca. Para evitar esse tipo de problema e preservar os estados quânticos é necessário isolar bem o sistema do resto do mundo. Essa tarefa não é tão complicada para sistemas pequenos, entretanto para sistemas maiores torna-se muito difícil. Para contornar esse problema podemos usar a teoria de informação quântica.

Durante uma computação clássica são cometidos pequenos erros que passam desapercebidos por-

que são monitorados e corrigidos através de códigos corretores de erros antes que o resultado chegue ao receptor. Porém, a decoerência dificulta que um processo semelhante possa ser feito no caso quântico, pois qualquer observação durante o processo destrói a superposição.

Em teoria esse problema pode ser solucionado através dos *códigos quânticos corretores de erros* (ou simplesmente QECC). A correção quântica de erros mostra que a teoria da informação quântica é um referencial útil para estudar o mundo, pois são necessários esquemas para anular as perturbações que podem destruir os frágeis estados quânticos. A construção de tais códigos está fortemente baseada nas propriedades de códigos lineares clássicos. Shor propôs o primeiro QECC, um análogo quântico para o código de repetição clássico, [70]. Independentemente outro código quântico foi proposto por Steane em [72]. Esses códigos foram depois aprimorados pelos *códigos CSS*, definidos por Calderbank e Shor, [15], e Steane [73]. Em [38], Gottesman propõe uma classe de códigos mais abrangente chamada *códigos estabilizadores*, da qual os códigos CSS fazem parte. Veremos mais sobre esses códigos nas seções 3.4 e 3.5. Muitos outros trabalhos nessa área estão sendo desenvolvidos desde que Shor possibilitou a correção quântica de erros.

Esse modelo de computação quântica é baseado no modelo adotado pela computação clássica, mas existem outros modelos tais como, computação quântica baseada em medidas e computação quântica adiabática, [32].

Atualmente, as pesquisas na área de computação quântica se dividem em dois caminhos: a construção de um computador quântico real e a formulação dos programas que serão executados nesse computador. Nesta última, muitas pesquisas estão sendo desenvolvidas em busca de algoritmos, protocolos de criptografia e correção de erros. Quanto à construção de um computador quântico, o otimismo inicial sofreu um certo abalo devido às dificuldades para contornar os problemas de fragilidade da informação quântica e o caráter quase inevitável de erros de inicialização. Porém houve vários avanços na construção dos primeiros protótipos. Hoje a computação quântica se encontra num ponto semelhante ao que se encontrava a computação clássica na década de 1930. Muitas tecnologias estão sendo estudadas, mas ainda não há uma proposta completamente definida.

De qualquer maneira, seja qual for a proposta experimental para a construção de um computador quântico, esta deve satisfazer duas condições básicas: permitir acesso ao sistema e impedir que interações com o ambiente venham a destruir rapidamente as superposições. Além dessas condições, existem também outros problemas como, por exemplo, fazer com que o sistema seja escalonado. As principais propostas experimentais que estão sendo atualmente investigadas são: os pontos quântico, ressonância magnética nuclear, átomos de fósforo de silício, armadilhas de íons, supercondutores, entre outras. Para um aprofundamento neste assunto sugerimos as referências [14, 32, 56].

Enquanto isso, podemos começar a desfrutar de algumas tecnologias associadas a essa pesquisa bem antes de conseguirmos construir um computador quântico de porte. Algumas delas são: a criação e uso de partículas emaranhadas que permitem a utilização da criptografia quântica com segurança absoluta, também estão sendo testados vários outros protocolos de comunicação que utilizam sistemas quânticos de modo eficiente, e a produção de materiais e dispositivos sofisticados em escala nanoscópica que estão sendo produzidos, [32].

Apesar de todas as dificuldades que a computação quântica tem enfrentado, não há como negar sua importância e a necessidade de que as pesquisas continuem. A principal motivação é que em um computador quântico poderemos simular sistemas quânticos. Esse problema é fundamental para áreas como química e nanotecnologia, e sua importância pode ser comprovada se observarmos que alguns Prêmios Nobel têm sido concedidos mesmo para avanços parciais nessa área, [67]. Além dessa inquestionável aplicação, ainda temos os ganhos computacionais promovidos pelos algoritmos de Shor e Grover.

Vale lembrar que apesar das aparentes limitações desses computadores, não há nenhuma razão que demonstre sua inviabilidade. Finalizamos essa seção citando Scott em [67]: "As limitações aumentam nossa crença de que a computação quântica será possível afinal - porque quanto mais uma tecnologia proposta se parece com uma caricatura da ficção científica, mais céticos nos tornamos".

3.2 Mecânica Quântica

"Pode-se dizer com segurança que ninguém entende a mecânica quântica."

-Richard Feynman

As teorias físicas baseadas nos estudos de Newton, e outros pesquisadores, conhecida agora como *física clássica* ou *mecânica clássica*, não foram eficazes ao tentar explicar a natureza do mundo em escala atômica. Isso porque objetos tão pequenos são diferentes de objetos grandes aos quais a física clássica está acostumada. O ponto a partir do qual um objeto é considerado "pequeno" e seu comportamento torna-se diferente, depende de uma propriedade fundamental da Natureza, a constante universal $\hbar$ conhecida como *constante de Planck*, que aparece na maioria das equações quânticas.

Ao contrário da mecânica clássica, a mecânica quântica não é intuitiva, parece estar em desacordo com o que estamos acostumados a observar. No entanto, é a única teoria capaz de explicar o comportamento da matéria em escala atômica, e além disso, muitas previsões dessa teoria se aplicam também com sucesso a objetos macroscópicos, o que torna o domínio de aplicação da mecânica quântica muito maior do que o mundo microscópico.

Nesta seção descreveremos os principais aspectos de duas propriedades fundamentais da mecânica quântica que são importantes para a computação quântica, a saber a *superposição* e o *emaranhamento*.

3.2.1 A propriedade da superposição

Conhecemos a *interferência* como uma propriedade das ondas, que ocorre quando perturbações de diferentes fontes se encontram e se combinam somando em algumas regiões e subtraindo ou cancelando em outras. Essas perturbações são também chamadas *amplitudes*. A interferência requer distribuições extensas e sobrepostas. A física clássica descreve as partículas como algo com posição bem-definida e que não produzem interferência. Ao passo que na física quântica as partículas são descritas como ondas, e podem apresentar os efeitos da interferência.

Quando um resultado pode ser obtido por várias maneiras diferentes, uma *amplitude* é associada a cada uma dessas possíveis maneiras. A amplitude pode ser positiva ou negativa, com os diferentes percursos podendo se somar ou subtrair, até mesmo se anular, uns com os outros e resultar em interferência, como ocorre com as ondas. Por esse motivo, a amplitude é freqüentemente chamada *função onda*.

Ao multiplicar a amplitude por si mesma, obtemos uma *distribuição de probabilidades*, que indica qual a probabilidade de uma partícula se encontrar em uma determinada posição. Se as diferentes amplitudes se combinam em certas regiões, então aumenta a probabilidade de se encontrar partículas nessas regiões. Por outro lado, se em alguns lugares as amplitudes se cancelam mutuamente, então a probabilidade de se encontrar partículas nesses lugares diminui. A menos que a probabilidade seja zero, e nesse caso pode-se dizer com certeza que a partícula não se encontra nesse estado, não é possível dizer em que estado a partícula estará. Porém, se existir um número muito grande de partículas, é possível dizer com bastante precisão o lugar onde essas partículas estão.

Em suma, a mecânica quântica se refere a partículas como *estados* e *amplitudes*. Quando se eleva ao quadrado uma amplitude, obtém-se uma *distribuição de probabilidade* que fornece a *probabilidade* de se obter um dos vários resultados ao se fazer uma *observação*. O valor obtido em cada observação parece ser aleatório e imprevisível, mas se forem feitas muitas observações, o resultado médio pode ser previsto com precisão.

Uma *superposição de estados* é obtida quando se soma todas as amplitudes. Isso significa que a partícula está fazendo tudo o que é possível. Classicamente, isso é um fato contraditório. É como se a partícula pudesse estar simultaneamente em várias posições diferentes. Além disso, a interferência mostra que as probabilidades estão todas presentes e influenciam umas às outras.

O sistema fica numa superposição de estados até que uma *observação* ou *medida* seja feita, ou seja,

até que se olhe o que o sistema está fazendo. Ao se fazer isso, uma única possibilidade é selecionada e esta será a única ocorrência do sistema. Todas as outras possibilidades que estavam acontecendo no sistema simplesmente desaparecem, ou se anulam, e o estado observado passa a ser o único real. Mas a possibilidade observada não é obtida através de uma escolha. Na verdade, ela é determinada pelas probabilidades dos vários estados quânticos. As amplitudes proporcionam as probabilidades dos diferentes resultados, mas não estabelecem o que vai acontecer. Isso é puro acaso, e somente é fixado após feita uma observação.

A seleção de uma única possibilidade e a redução de todas as outras amplitudes, é conhecido como o *problema da medida*. Este é um problema muito diferente de outros comportamentos quânticos, e existem várias "respostas" para ele, mas nenhuma é universalmente aceita. Convencionalmente, a mecânica quântica afirma que quando for possível que coisas diferentes aconteçam em um sistema físico, haverá uma amplitude associada a cada uma dessas possibilidades e a soma de todas as amplitudes resulta em uma superposição de estados, podendo haver interferência entre as amplitudes individuais. Não havendo influências externas, as amplitudes se alterarão de maneira suave e previsível de modo que ao se fazer uma medida chega-se a um valor correspondente a uma dessas amplitudes e as demais desaparecerão. Imediatamente após a medida, o valor da amplitude passa a ser uma quantidade conhecida.

Assim, a superposição, uma das principais características de objetos microscópicos que seguem as regras da mecânica quântica, é a possibilidade de um objeto quântico assumir uma combinação peculiar de probabilidades que seriam mutuamente excludentes de acordo com a nossa intuição clássica. Pode-se dizer que na mecânica quântica tudo que não é proibido, é compulsório, inclusive processos classicamente impossíveis, tais como a penetração de partículas através de uma estreita barreira de energia. Esse fato é possível porque a amplitude associada a possibilidade de uma partícula penetrar tal barreira não é nula, apesar de ser menor. Isso dá margem a uma pequena probabilidade para que a partícula possa aparecer do outro lado da barreira, tendo aparentemente atravessado uma barreira aparentemente intransponível, esse processo é chamado *tunelamento*.

Depois de definir a superposição, vejamos como essa característica quântica pode ajudar na computação. Na computação clássica temos apenas dois estados, 0 e 1, e apenas um deles pode ser usado por vez. Já na computação quântica, a superposição nos permite ser mais versáteis. Temos vários estados que podem ser usados simultaneamente até que seja feita uma medida. Isso possibilita processamentos fortemente paralelos. Entretanto, para que essa propriedade seja usada com eficiência é preciso manipular esse estado de superposição para que o resultado da medida traga ganho computacional. Em geral, as manipulações vão alterar as amplitudes associadas a cada posição, e a medida final

vai revelar a partícula em alguma das posições com uma probabilidade que só depende das amplitudes de probabilidades imediatamente antes da medida. Enquanto evitarmos medir a posição, essas amplitudes "fluem" da maneira que quisermos, assim como uma onda pode mudar de forma. Ao medirmos a posição destruímos a superposição, e a partícula volta a se comportar classicamente. Enfatizamos que uma partícula nunca aparece dividida entre posições, mas sempre em uma posição ou na outra, como é esperado que uma partícula faça.

O algoritmo de Shor é um exemplo do uso eficiente de manipulações em um estado de superposição, e é devido a isso que este algoritmo oferece um ganho computacional de ordem exponencial.

Ao mesmo tempo que as superposições podem fornecer vantagem computacional, foi visto na Seção 3.1 que a decoerência é uma das principais dificuldades na construção de computadores quânticos.

Para que essa vantagem seja de fato aproveitada é necessário entender como um número relativamente pequeno de operações quânticas pode ser equivalente a um número muito maior de passos computacionais clássicos. A manipulação do estado de superposição, que é um passo computacional absolutamente quântico, está por trás desse fato.

Exemplo 3.1 *Neste exemplo consideramos partículas como elétrons e fótons para compreender algumas propriedades das partículas.*

Elétrons (ou fótons) têm associados a eles uma função onda, ou amplitude, e esta amplitude é uma superposição de todas as coisas que essas partículas poderiam estar fazendo. No entanto, tais partículas são totalmente idênticas umas com as outras, e por isso não há como saber quando dois elétrons (ou fótons) permutaram. Isso significa que a função onda total será uma superposição de todas as amplitudes para as quais um par diferente tenha sido trocado.

Sabemos que a probabilidade de se fazer uma observação é dada pelo quadrado da sua função onda então, é claro que este valor não será alterado quando duas partículas são permutadas. Entretanto, já foi dito que a amplitude pode ser positiva ou negativa, isso significa que a amplitude pode mudar de sinal quando duas partículas trocam de lugar e ainda assim a probabilidade não ser alterada. É como multiplicar a amplitude por -1*. A mudança de sinal parece um detalhe sem maiores consequências, mas isso não é totalmente verdade. As partículas para as quais a amplitude muda de sinal quando duas delas são permutadas, são chamadas* **férmions***. Um exemplo de partículas do tipo férmion são os elétrons. Há também as partículas cujas amplitudes não mudam nunca quando elas são permutadas, essas são conhecidas como* **bósons***. Os fótons são exemplos de bósons. O fato do sinal de uma amplitude mudar ou não quando duas partículas trocam de estado realmente importa para um sistema de partículas. Isso porque, devido ao Princípio de Exclusão de Pauli, não se pode*

ter dois férmions no mesmo estado. Por exemplo, os elétrons podem ser de dois tipos: **spin-up** *e* **spin-down**. *De acordo com o princípio de exclusão de Pauli se um estado já tiver um spin-up, no mesmo estado só poderá haver mais um spin-down. O spin pode ser usado para codificar bits quânticos. Ao contrário dos férmions, os bósons não obedecem a esse princípio, e portanto, se dois bósons estiverem no mesmo estado e permutarem de lugar, realmente não fará diferença alguma.*

Mais informações sobre partículas elementares pode ser encontrada em [1].

3.2.2 A propriedade de emaranhamento

Nesta subseção apresentamos uma das mais inacreditáveis características quânticas, o *emaranhamento*. Tal característica possibilita a criação de conjuntos de partículas que apresentam fortes correlações entre suas propriedades. A essa propriedade é dado o nome de *não-localidade quântica*, um termo que indica que os resultados parecem depender do que está sendo medido em vários locais ao mesmo tempo.

Estados emaranhados são caracterizados por serem bem definidos apenas como um todo, ou seja, todas as suas propriedades estão armazenadas nas características globais do estado, e não em cada partícula individual, não importando a distância entre eles. Assim, qualquer interação com um estado emaranhado, como por exemplo, uma medida, afeta simultaneamente tudo que está emaranhado com ele. A definição formal de emaranhamento quântico é dada na próxima seção, pois é necessário algumas definições e notações que só serão apresentadas lá.

O emaranhamento é um recurso físico quantificável que permite executar tarefas de processamento de informações. A importância dada a essa propriedade é comparada a importância da energia, da informação, da entropia ou de qualquer outro recurso fundamental da Natureza. Ainda não existe uma teoria completa sobre emaranhamento, porém os progressos feitos nesse estudo apontam na direção de aplicações surpreendentes na computação e informação quântica, [56].

Uma das principais aplicações do emaranhamento está relacionada à criptografia quântica, que explora a não-localidade quântica para transmitir mensagens com segurança absoluta. Outra aplicação é no teletransporte quântico, como vimos na seção anterior. Há ainda aplicações em codificação de dados de forma mais robusta contra erros, sincronização mais eficiente de relógios distantes, autenticação bancária, etc.

3.3 Informação e Computação Quântica

"Information is physical."

-Rolf Landauer.

Ao contrário do que possa parecer, a informação não é algo abstrato, ou puramente matemático. A informação é uma entidade concreta, uma manifestação física. A concretude da informação quântica respeita as leis da física quântica, assim como a informação clássica respeita as leis da física clássica. No entanto, por esse ser um assunto ainda em desenvolvimento, existe uma confusão no que diz respeito ao conceito de informação quântica. O termo "informação quântica" é usado tanto para as operações relacionadas com o processamento da informação por meio da mecânica quântica, como também para o estudo das tarefas básicas no processamento da informação quântica. O primeiro caso inclui aplicações tecnológicas como computação quântica, teletransporte quântico, entre outros. Já o segundo, é análogo ao termo "teoria da informação clássica", [56].

Nesta seção apresentamos a unidade fundamental da informação quântica e suas interpretações, bem como a execução da computação quântica através de portas lógicas quânticas. Para isso, fazemos uma revisão de alguns conceitos de álgebra linear.

3.3.1 O bit quântico

A unidade fundamental da informação clássica é o *bit*, que pode assumir dois estados: 0 ou 1. Analogamente, a unidade da informação quântica é o *bit quântico* ou *qubit* que pode assumir dois estados: $|0\rangle$ e $|1\rangle$, e como vimos na seção anterior, também pode existir em uma superposição dos estados $|0\rangle$ e $|1\rangle$. A notação "$|\cdot\rangle$" é conhecida como *notação de Dirac*, e nesta forma recebe o nome de *ket*. Apesar de parecer incomum para matemáticos e engenheiros, essa notação para estados quânticos adotada pelos físicos é padrão.

Os qubits são objetos físicos. Por exemplo, um qubit pode ser uma partícula como um elétron, onde um *spin up* representa o estado $|1\rangle$, um *spin down* representa o estado $|0\rangle$, e os estados em superposição de $|0\rangle$ e $|1\rangle$ envolvem simultaneamente *spin up* e *spin down*, [67]. Entretanto, iremos descrever os qubits como objetos matemáticos com certas propriedades. Assim, a teoria geral não dependerá de nenhum sistema quântico específico.

Matematicamente, um qubit é um vetor em um espaço vetorial complexo bidimensional com produto interno, ou seja, um vetor no espaço de Hilbert. Uma maneira de representar um qubit é através de uma seta apontando para um local sobre uma esfera. Essa esfera é conhecida como *esfera de Bloch* (Figura 3.1). Enquanto bits são representados apenas como uma seta apontando para cima no caso do estado 1, e uma seta apontando para baixo para indicar o estado 0, na esfera de Bloch o pólo norte equivale ao estado $|1\rangle$, o pólo sul equivale ao estado $|0\rangle$, e os outros locais na esfera são as superposições dos estados $|0\rangle$ e $|1\rangle$, [55]. A esfera de Bloch permite a visualização de muitas operações sobre qubits

isolados, porém não existe uma generalização simples da esfera de Bloch para muitos qubits, [56].

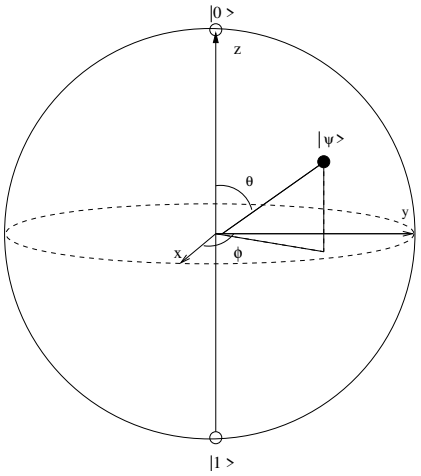

Figura 3.1: Esfera de Bloch.

A propriedade da superposição faz parecer que um qubit pode conter uma quantidade infinita de informações, devido ao fato de suas coordenadas poderem codificar uma sequência infinita de dígitos. No entanto, essa conclusão é falsa, pois não há como extrair essa informação do qubit. Independentemente do tipo de mensuração, a medida de um qubit resultará sempre em um estado $|0\rangle$ ou $|1\rangle$. Se o qubit estiver em um estado de superposição, a medida o fará colapsar para algum estado específico. Mesmo assim, foi visto que essa propriedade é muito importante para a computação quântica.

Um estado de superposição para um qubit pode ser escrito na forma

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

onde $\alpha, \beta \in \mathbb{C}$ são as amplitudes dos estados $|0\rangle$ e $|1\rangle$, respectivamente, e satisfazem a condição

$$|\alpha|^2 + |\beta|^2 = 1,$$

uma vez que $|\alpha|^2$ e $|\beta|^2$ são as probabilidades de se encontrar os estados $|0\rangle$ e $|1\rangle$, respectivamente, ao se medir o qubit $|\psi\rangle$, e como sabemos, a soma das probabilidades deve ser sempre igual a um.

Essa superposição de estados significa que o estado $|\psi\rangle$ está simultaneamente nos estados $|0\rangle$ e $|1\rangle$. Após a medida, o estado deve colapsar para $|0\rangle$ ou $|1\rangle$ com suas respectivas probabilidades.

Os estados $|0\rangle$ e $|1\rangle$ formam uma base ortonormal de $\mathbb{C}^2$, chamada *base computacional*.

Classicamente, ao considerar dois bits, obtemos quatro estados diferentes: $00, 01, 10, 11$, que correspondem respectivamente às representações binárias dos números $0, 1, 2$ e 3. Analogamente, um sistema quântico com dois qubits possui quatro estados na base computacional: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Além disso, um par de qubits pode existir também em superposição desses quatro estados da seguinte forma

$$|\eta\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

com

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

No caso geral, o estado $|v\rangle$ com n qubits, é uma superposição dos 2^n estados $|00\ldots0\rangle$, $|00\ldots1\rangle$, $\ldots, |11\ldots1\rangle$, onde a sequência dentro de cada *ket* é a representação binária dos números $0, 1, \ldots, 2^n - 1$, e portanto, também pode ser escrita resumidamente como $|0\rangle$, $|1\rangle$, $\ldots$, $|2^n - 1\rangle$. Assim,

$$|v\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle,$$

com a restrição

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

O estado $|v\rangle$ pertence ao espaço vetorial complexo 2^n dimensional.

3.3.2 Álgebra linear

Nesta subseção faremos uma breve revisão de alguns conceitos básicos de álgebra linear sob a notação padrão utilizada na mecânica quântica. Para um aprofundamento maior nesse assunto sugerimos as referências [56, 64, 78].

Os estados $|0\rangle$ e $|1\rangle$ podem ser representados na forma matricial da seguinte maneira:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

A superposição $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, também pode ser escrita em forma de matriz,

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

A representação matricial é conveniente para compreender as operações que estão sendo realizadas, porém quando temos muitos qubits fica impraticável escrever em forma de matriz.

Em seguida definiremos operadores lineares e as principais características relacionadas a eles, além das operações de produto interno e produto tensorial.

Definimos um *operador linear* entre os espaços vetoriais V e W como uma aplicação $A : V \to W$, linear na sua ação:

$$A(\sum_i a_i|v_i\rangle) = \sum_i a_i A(|v_i\rangle).$$

Em geral, usa-se $A|v\rangle$ para denotar $A(|v\rangle)$. Dizemos que um operador linear A é definido no espaço vetorial V, se A é um operador linear de V em V. O operador identidade I_V é definido pela equação $I_V|v\rangle \equiv |v\rangle$ para todo $|v\rangle \in V$. A composição de dois operadores $A : V \to W$ e $B : W \to X$, onde V, W e X são espaços vetoriais, é dada por $(BA)|v\rangle = B(A|v\rangle) = BA|v\rangle$.

Uma maneira equivalente, e mais conveniente, de descrever os operadores lineares é através de suas representações matriciais. Seja $A : V \to W$ um operador linear entre os espaços vetoriais V e W, e suponha que $\{|v_1\rangle, |v_2\rangle, \ldots, |v_m\rangle\}$ e $\{|w_1\rangle, |w_2\rangle, \ldots, |w_n\rangle\}$ sejam bases de V e W, respectivamente. Então, para cada $j \in \{1, 2, \ldots, m\}$ existem números complexos $A_{1j}, A_{2j}, \ldots A_{nj}$ tais que $A|v_j\rangle = \sum_i A_{ij}|w_i\rangle$. Assim, a matriz correspondente ao operador A é aquela cujas entradas são os valores A_{ij}.

Os principais operadores para um qubit são conhecidos como *matrizes de Pauli*, e são representados por

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X \equiv \sigma_x \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y \equiv \sigma_y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \equiv \sigma_z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Esses operadores formam um grupo multiplicativo não-abeliano $\mathscr{G}$. Veremos a importância desses operadores durante todo o trabalho.

Chamamos atenção para a notação de Dirac para um vetor dual. O dual de um vetor $|v\rangle \in \mathbb{C}^n$ é o vetor transposto de $|v\rangle$ cujos elementos são trocados pelos seus conjugados, e é denotado por $\langle v|$ que é a notação de Dirac conhecida como *bra*. Assim,

$$\langle v| = (|v\rangle)^\dagger,$$

onde † significa a conjugação transposta.

Como foi mencionado, um qubit é um vetor em um espaço vetorial complexo bidimensional com produto interno. Considere V um espaço vetorial e $|v\rangle, |w\rangle \in V$. Definimos o produto interno $\langle \cdot | \cdot \rangle : V \times V \to \mathbb{C}$ por

$$\langle v|w\rangle = (|v\rangle)^\dagger |w\rangle.$$

A *norma* de um estado $|v\rangle$ é então definida por

$$|| \, |v\rangle || = \sqrt{\langle v|v\rangle}.$$

Os espaços de interesse para a computação quântica e informação quântica são espaços vetoriais complexos de dimensão finita dotados de produto interno, ou seja, espaços de Hilbert. Portanto, os

dois termos, espaço vetorial com produto interno e espaço de Hilbert, serão usados como termos equivalentes no restante do trabalho.

Operadores lineares também podem ser representados através do produto interno usando o que é conhecido como "representação de produto externo". Seja $|v\rangle$ e $|w\rangle$ vetores dos espaços vetoriais com produto interno V e W, respectivamente. O operador linear $|w\rangle\langle v|$ de V em W é dado por:

$$(|w\rangle\langle v|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle.$$

Um *autovetor* de um operador linear A em um espaço vetorial é um vetor não-nulo $|v\rangle$ tal que $A|v\rangle = \lambda|v\rangle$, onde λ é um número complexo conhecido como *autovalor* de A, correspondente a $|v\rangle$. Todo operador A tem pelo menos um autovalor e um autovetor correspondente. O *autoespaço* correspondente a um autovalor λ é o conjunto de vetores com autovalores λ acrescido do vetor nulo. Verifica-se que esse é um subespaço vetorial do espaço onde A atua.

Uma *representação diagonal* de um operador A em um espaço vetorial V é uma representa-ção $A = \sum_i \lambda_i |i\rangle\langle i|$, em que os vetores $|i\rangle$ formam um conjunto de autovetores ortogonais de A, com autovalores correspondentes λ_i. Um operador é dito *diagonalizável* se possui uma representação diagonal.

Definição 9 *Seja A um operador linear no espaço de Hilbert $\mathscr{H}$. Chamamos de operador adjunto ou conjugado Hermitiano de A em $\mathscr{H}$, e denotado por $A^\dagger$, o único operador tal que para todos os vetores $|v\rangle, |\omega\rangle \in \mathscr{H}$,*

$$(|v\rangle, A|\omega\rangle) = (A^\dagger|v\rangle, |\omega\rangle).$$

Da definição, segue que $(AB)^\dagger = B^\dagger A^\dagger$. Por convenção, o adjunto de um vetor $|v\rangle$ é $|v\rangle^\dagger \equiv \langle v|$. Assim, $(A|v\rangle)^\dagger = \langle v|A^\dagger$. Note também que, $(A^\dagger)^\dagger = A$.

Em termos de representação matricial de um operador A, a conjugação Hermitiana transforma a matriz de A em sua conjugada transposta, ou seja, em $A^\dagger = (A^*)^T$, onde "$*$" indica conjugação complexa e "T" é a operação de transposição. Por exemplo,

$$\begin{bmatrix} 1+2i & 2i \\ 2+i & -1 \end{bmatrix}^\dagger = \begin{bmatrix} 1-2i & 2-i \\ -2i & -1 \end{bmatrix}.$$

Definição 10 *Dizemos que um operador linear A é Hermitiano ou auto-adjunto se $A = A^\dagger$.*

Destacamos uma importante classe de operadores Hermitianos conhecida como *projetores*. Seja V um espaço vetorial com dimensão d e W um subespaço de V com dimensão k. Usando o processo de

Gram-Schmidt é possível construir uma base ortonormal $|1\rangle, |2\rangle, \ldots, |d\rangle$ de V, tal que $|1\rangle, |2\rangle, \ldots |k\rangle$ seja uma base ortonormal de W. Definimos o projetor sobre W por

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i|.$$

Pode-se verificar que esta definição independe da base $|1\rangle, |2\rangle, \ldots |k\rangle$ de W. Da definição segue que, $|v\rangle\langle v|$ é Hermitiano para qualquer $|v\rangle$, de modo que P é Hermitiano. O *complemento ortogonal* de P é o operador $Q \equiv I - P$ que é um projetor sobre o espaço $|k+1\rangle, \ldots |d\rangle$. A ação de projeção de P resultará no processo de medida quântica.

Diz-se que um operador A é *normal* se $A^\dagger A = AA^\dagger$. Assim, um operador Hermitiano é normal. Se um operador A é tal que $A^\dagger A = AA^\dagger = 1$, então esse operador é dito *unitário*. Note que, os operadores de Pauli são Hermitianos e unitários.

Definiremos abaixo o *produto tensorial*, que é uma forma de juntar espaços vetoriais para obter um outro espaço vetorial maior. Esse procedimento é muito útil para a descrição da mecânica quântica de sistemas com muitas partículas.

Sejam V e W espaços de Hilbert de dimensões m e n, respectivamente. O produto tensorial $V \otimes W$ é um espaço vetorial de dimensão mn, cujos elementos são combinações lineares de produtos tensoriais $|v\rangle \otimes |w\rangle$ dos elementos $|v\rangle \in V$ e $|w\rangle \in W$. Em particular, o produto tensorial de bases ortonormais de V e W é uma base de $V \otimes W$. Pode-se escrever $|vw\rangle$ ou $|v\rangle|w\rangle$ em vez de $|v\rangle \otimes |w\rangle$.

Considere V e W espaços vetoriais. O produto tensorial deve satisfazer as seguintes propriedades:

- $z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$, onde $|v\rangle \in V$, $|w\rangle \in W$ e $z \in \mathbb{C}$;
- $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle|w\rangle + |v_2\rangle|w\rangle$, onde $|v_1\rangle, |v_2\rangle \in V$ e $|w\rangle \in W$;
- $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle|w_1\rangle + |v\rangle|w_2\rangle$, onde $|v\rangle \in V$ e $|w_1\rangle, |w_2\rangle \in W$.

Se A e B são operadores, respectivamente, em V e W, pode-se definir o operador $A \otimes B$ em $V \otimes W$ por

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle,$$

para todos os elementos $|v\rangle \otimes |w\rangle \in V \otimes W$. Mostra-se que $A \otimes B$ é de fato um operador linear atuando em $V \otimes W$. Além disso, qualquer operador linear $C : V \otimes W \to V' \otimes W'$ pode ser representado como uma combinação linear de produtos tensoriais de operadores $A : V \to V'$ e $B : W \to W'$. Pode-se usar os produtos internos definidos em V e W para definir o produto interno em $V \otimes W$:

$$(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle) = \sum_{ij} a_i^* b_j \langle v_i|v'_j\rangle\langle w_i|w'_j\rangle.$$

Todas as outras noções como operador adjunto, unitário e Hermitiano, são naturalmente estendidas para $V \otimes W$.

Ainda introduzindo algumas notações, $|\psi\rangle^{\otimes n}$ e $A^{\otimes n}$ significam os produtos tensoriais de $|\psi\rangle$ e de A, por eles mesmos n vezes.

Essa discussão sobre produto tensorial pode se tornar mais clara usando uma representação matricial conhecida como *produto de Kronecker*.

Definição 11 *Considere as matrizes $A_{m\times n}$ e $B_{p\times q}$. O produto tensorial de A e B é dado pela matriz de ordem $mp \times nq$*

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix},$$

onde A_{ij} é o elemento localizado na linha i e coluna j da matriz A e cada termo $A_{ij}B$ denota uma sub-matriz $p \times q$ cujos elementos são os produtos de A_{ij} por cada elemento da matriz B.

O produto tensorial não é comutativo. Por exemplo,

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

enquanto

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Outra definição importante que será usada nos próximos capítulos se refere às relações de comutação entre os operadores lineares.

Definição 12 *Sejam A e B dois operadores lineares em um mesmo espaço vetorial. Definimos o comutador entre A e B como*

$$[A,B] = AB - BA.$$

Se $[A,B] = 0$, dizemos que A e B comutam. Analogamente, podemos definir o anticomutador como

$$\{A,B\} = AB + BA.$$

Se $\{A,B\} = 0$, dizemos que A e B anticomutam.

O comutador e o anticomutador nos proporcionam algumas importantes propriedades de pares de operadores. Talvez a principal seja a conexão entre o comutador e a propriedade de diagonalização simultânea de operadores.

Teorema 4 (Teorema da diagonalização simultânea) [56] *Sejam A e B operadores Hermitianos.* $[A,B]=0$ *se, e somente se, existir uma base ortonormal tal que A e B sejam ortonormais nesta base. Neste caso, diz-se que A e B são simultaneamente diagonalizáveis.*

Ou seja, duas matrizes que comutam entre si são simultaneamente diagonalizáveis. Assim, podemos medir o autovalor de uma delas sem destruir os autovetores da outra.

Pode-se verificar facilmente que as relações de comutação para os operadores de Pauli são:

$$[\sigma_x,\sigma_y]=2i\sigma_z,\ \ [\sigma_y,\sigma_z]=2i\sigma_x,\ \ [\sigma_z,\sigma_x]=2i\sigma_y.$$

E as relações de anticomutação para os mesmos são:

$$\{\sigma_i,\sigma_j\}=0$$

para $i\neq j$, $i=1,2,3$.

Como havia sido prometido na subseção 3.2.2, abaixo definimos formalmente um emaranhamento quântico.

Um estado de dois qubits pode ou não ser o resultado do produto tensorial de estados de um qubit. Considere os estados de um qubit $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ e $|\varphi\rangle=\gamma|0\rangle+\delta|1\rangle$, onde $\alpha,\beta,\gamma,\delta\in\mathbb{C}$. O estado definido pelo produto tensorial de $|\psi\rangle$ e $|\varphi\rangle$ é:

$$\begin{aligned}|\psi\rangle\otimes|\varphi\rangle &= (\alpha|0\rangle+\beta|1\rangle)\otimes(\gamma|0\rangle+\delta|1\rangle)\\ &= \alpha\gamma|00\rangle+\alpha\delta|01\rangle+\beta\gamma|10\rangle+\beta\delta|11\rangle. \qquad (3.1)\end{aligned}$$

Um estado de dois qubits genérico $a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle$ é da forma 3.1 se, e somente se,

$$a=\alpha\gamma,\quad b=\alpha\delta,$$

$$c=\beta\gamma,\quad d=\beta\delta.$$

Segue que,

$$\frac{b}{d}=\frac{\alpha}{\beta}=\frac{a}{c}.$$

Assim, $ad = bc$. Portanto, um estado de dois qubits, em geral, não é o produto tensorial de estados de um qubit. Quando isso acontece, dizemos que o estado está emaranhado. Por exemplo, o estado $|10\rangle$ pode, obviamente, ser descrito como o produto tensorial dos estados $|1\rangle$ e $|0\rangle$,

$$|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Por outro lado, o estado

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

é um estado emaranhado, pois não pode ser escrito como produto tensorial de estados de um qubit.

Os mais famosos estados emaranhados de dois qubits são:

$$\beta_{|00\rangle} = \frac{1}{2}(|00\rangle + |11\rangle),$$
$$\beta_{|10\rangle} = \frac{1}{2}(|00\rangle - |11\rangle),$$
$$\beta_{|01\rangle} = \frac{1}{2}(|01\rangle + |10\rangle),$$
$$\beta_{|11\rangle} = \frac{1}{2}(|01\rangle - |10\rangle),$$

conhecidos como estados de Bell ou pares EPR (Einstein - Podolsky - Rosen). Estes estados servem como unidade básica de emaranhamento em muitas aplicações de criptografia quântica.

Em geral, um estado $|v\rangle$ em um espaço vetorial é dito emaranhado se não puder ser escrito como produto tensorial de estados de um qubit. Por exemplo, o estado

$$|\xi\rangle = \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

é um estado emaranhado. Já o estado

$$|\zeta\rangle = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

é não emaranhado porque pode ser decomposto em

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes [1 \;\; 0] \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes [0 \;\; 1].$$

Para n qubits, um estado emaranhado, conhecido como *estado GHZ*, é dado por

$$\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle).$$

3.3.3 Portas quânticas

Assim como os circuitos de computadores clássicos contém fios e portas lógicas que transportam e manipulam a informação, um computador quântico é construído a partir de um circuito quântico contendo também fios e portas lógicas quânticas que transportam e manipulam a informação quântica de um lado para outro.

A inicialização da computação quântica é feita com a preparação de alguns qubits iniciais com os dados de entrada do problema. As portas lógicas sobre o sistema quântico operam sequencialmente nos qubits de acordo com o algoritmo, mudando as amplitudes que descrevem a superposição. Depois da aplicação das portas lógicas, o resultado da computação é obtido através de medidas em alguns qubits pré-escolhidos.

Para um bit clássico, a única porta não trivial é conhecida como porta NOT cuja operação transforma 0 em 1, e 1 em 0. Para muitos bits clássicos, temos as portas lógicas AND, OR, XOR, NAND e NOR, cujas ações são descritas na Tebela 3.1. Um importante resultado mostra que qualquer função sobre bits pode ser computada a partir da composição somente de portas NAND, portanto dizemos que esta é uma porta *universal*.

bit de entrada	AND	OR	XOR	NAND	NOR
00	0	0	0	1	1
01	0	1	1	1	0
10	0	1	1	1	0
11	1	1	0	0	0

Tabela 3.1: Portas lógicas para dois bits.

No caso quântico também temos a porta NOT dada pela matriz de Pauli X, conhecida como operador *bit flip*, que transforma $|0\rangle$ em $|1\rangle$ e $|1\rangle$ em $|0\rangle$. A ação de X no estado de superposição $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ é linear, assim $X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$, ou matricialmente

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

A propriedade linear é geral na mecânica quântica, e muito bem embasada experimentalmente. Do contrário, comportamentos não-lineares poderiam levar a paradoxos tais como viagens no tempo, comunicação mais rápida do que a luz e violação das leis da termodinâmica, [56].

Podemos descrever as portas quânticas sobre um qubit por matrizes 2×2. É importante observar que a condição $|\alpha|^2 + |\beta|^2 = 1$ para um estado quântico $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ também deve ser satisfeita pelo estado $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ após a aplicação da porta lógica, ou seja, $|\alpha'|^2 + |\beta'|^2 = 1$. Portanto a

matriz que representa a porta lógica deve ser unitária. Essa é a única condição imposta sobre as portas quânticas. Assim, qualquer matriz unitária especifica uma porta lógica quântica.

Pode-se concluir que as matrizes de Pauli são portas lógicas quânticas. Em especial, a porta Z, conhecida como *operador phase flip*, age trocando o sinal do estado $|1\rangle$

$$\begin{aligned} Z|0\rangle &= |0\rangle \\ Z|1\rangle &= -|1\rangle. \end{aligned}$$

Não existe uma porta análoga a essa no caso clássico.

Outra porta para um qubit, muito importante, é conhecida como *porta de Hadamard*, cuja representação matricial é dada por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Essa porta transforma o estado $|0\rangle$ no estado $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e o estado $|1\rangle$ no estado $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Note que, qualquer estado $|\psi\rangle$ pode ser escrito em termos de $|+\rangle$ e $|-\rangle$, da seguinte maneira:

$$\frac{1}{\sqrt{2}}(\alpha+\beta)|+\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|-\rangle.$$

Assim, $\{|+\rangle, |-\rangle\}$ é uma base de $\mathbb{C}$ chamada *base conjugada*. Os vetores $|+\rangle$ e $|-\rangle$ são escritos matricialmente como

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

A porta de Hadamard H permite colocar um qubit num estado de superposição dos valores $|0\rangle$ e $|1\rangle$ com amplitudes iguais.

Na Tabela 3.2 mostramos como as portas para um qubit, X, Z e H, agem.

bit de entrada	X	Z	H
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$
$\|1\rangle$	$\|0\rangle$	$-\|1\rangle$	$\|-\rangle$

Tabela 3.2: Portas quânticas para um qubit.

Uma importante porta lógica quântica para mais de um qubit é a NOT-controlada, ou simplesmente CNOT. Essa porta tem dois qubits de entrada, conhecidos como *qubit de controle* e *qubit alvo*. A porta CNOT age no qubit alvo, trocando-o de $|0\rangle$ para $|1\rangle$ e de $|1\rangle$ para $|0\rangle$, se o qubit controle for o estado $|1\rangle$. Se o qubit controle for colocado no estado $|0\rangle$, nada acontece com o qubit alvo, veja Tabela 3.3.

Outra maneira de descrever a porta CNOT é vê-la como uma generalização da porta clássica XOR: $|a,b\rangle \rightarrow |a, b \oplus a\rangle$, onde $\oplus$ é a adição módulo 2. Também podemos representar a porta CNOT através

bit de entrada	CNOT
00	00
01	01
10	11
11	10

Tabela 3.3: Porta CNOT.

da matriz

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Note que essa matriz é unitária. O fato de qualquer porta quântica ser uma matriz unitária, implica que sua inversa também é uma matriz unitária, então elas são sempre reversíveis, ou seja, uma porta quântica pode sempre ser invertida por outra porta quântica.

Existem outras portas quânticas interessantes, porém esta porta é, sem dúvida, especial, pois qualquer porta lógica quântica de múltiplos qubits pode ser obtida a partir da porta CNOT e portas de um qubit. Portanto, a porta CNOT é universal.

Outro fato sobre a porta CNOT é que ela pode produzir um estado emaranhado. Considere o estado $|00\rangle$. Após a aplicação do operador $H \otimes I$ em $|00\rangle$, obtemos o estado $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$. Em seguida, aplicando neste estado a porta CNOT obtemos o estado de Bell $\beta_{|00\rangle}$.

3.4 Códigos Quânticos Corretores de Erros

Nesta seção apresentamos a *teoria dos códigos quânticos corretores de erros* (QECC), que protegem a informação quântica do ruído. O processamento da informação quântica é descrito como uma série de operações unitárias e medidas em alguns sistemas físicos. Foi visto na Seção 3.1 que interações com o ambiente em volta desses sistemas provocam a decoerência, além disso, imperfeições nas operações também podem prejudicar o processamento da informação. Para garantir que um computador quântico funcione de fato, temos que superar esses obstáculos. Para isso, foram desenvolvidas a *teoria dos códigos quânticos corretores de erros* e a *teoria da computação quântica tolerante à falhas*.

Os códigos quânticos corretores de erros funcionam codificando os estados quânticos de forma a torná-los resistentes à ação do ruído, e depois decodificando-os no momento em que se deseja recuperar os estados. Na subseção 3.4.1 revisamos os aspectos gerais da correção de erros e os desafios conceituais que devem ser superados no caso das correções quânticas de erros. A subseção 3.4.2 mos-

tra o código de Shor que é o exemplo mais simples de códigos quânticos corretores de erros e servirá para uma generalização dessa teoria na subseção 3.4.3. Por fim, na subseção 3.4.4 são apresentados os códigos CSS.

3.4.1 Desafios conceituais

Vimos no primeiro capítulo que, a idéia básica para proteger uma mensagem contra os efeitos do ruído em um canal é a adição de informação redundante. Assim, mesmo que alguma informação seja corrompida pelo ruído, é possível detectar e corrigir erros a ponto de recuperar a mensagem original.

Ainda neste capítulo, veremos que os QECC têm sua construção fortemente estruturada nos códigos lineares clássicos. Porém, existem algumas diferenças fundamentais entre informação clássica e informação quântica que deverão ser contornadas.

Uma dessas diferenças é a *impossibilidade de copiar um qubit*. No exemplo 2.1 é apresentado o código de repetição. Naturalmente, a primeira coisa a se pensar seria implementar o código de repetição quanticamente. No entanto, isso não é possível devido ao *teorema da não-clonagem*. Esse teorema afirma que é impossível fazer uma cópia perfeita de um estado quântico arbitrário desconhecido. De fato, suponha que tenhamos copiado os estados $|\psi\rangle$ e $|\varphi\rangle$, ou seja,

$$|\psi\rangle \longrightarrow |\psi\rangle \otimes |\psi\rangle \qquad |\varphi\rangle \longrightarrow |\varphi\rangle \otimes |\varphi\rangle.$$

Temos que,

$$|\psi\rangle + |\varphi\rangle \longrightarrow |\psi\rangle \otimes |\varphi\rangle + |\psi\rangle \otimes |\varphi\rangle.$$

Por outro lado,

$$|\psi\rangle + |\varphi\rangle \longrightarrow (|\psi\rangle + |\varphi\rangle) \otimes (|\psi\rangle + |\varphi\rangle).$$

Porém, $|\psi\rangle \otimes |\varphi\rangle + |\psi\rangle \otimes |\varphi\rangle \neq (|\psi\rangle + |\varphi\rangle) \otimes (|\psi\rangle + |\varphi\rangle)$.

Em geral, dada uma base ortonormal, é possível copiar os estados da base, mas não é possível copiar corretamente as superposições desses estados.

Outra diferença é que *em um único qubit podem ocorrer erros diferentes de forma contínua*. Ou seja, um erro no estado $\alpha|0\rangle + \beta|1\rangle$ pode mudar α e β por uma quantidade ε, e estes pequenos erros podem se acumular ao longo do tempo. Além disso, os erros do tipo *phase-flip* não ocorrem no caso clássico, esses são erros graves, pois podem transformar o estado $|+\rangle$ no estado $|-\rangle$.

Finalmente, a última diferença fundamental que destacaremos aqui, é que as *medidas destroem a informação quântica*. Na correção clássica de erro, é possível observar e corrigir erros na saída

do canal e decidir qual o procedimento a ser adotado. Enquanto a observação em mecânica quântica geralmente destrói o estado quântico sob observação, o que impossibilita sua recuperação.

Mesmo com essas diferenças, foi possível desenvolver a correção quântica de erros introduzindo novas idéias para que os códigos quânticos de correções de erros possam funcionar.

3.4.2 O código de Shor

Veremos agora alguns exemplos de códigos quânticos corretores de erros.

Um *código quântico corretor de erros* é uma função de um espaço de Hilbert 2^k-dimensional em um espaço de Hilbert 2^n-dimensional, onde $k < n$. As palavras-código são os vetores no espaço 2^n-dimensional. A *distância mínima d* de um QECC $\mathscr{C}$ é a menor distância de Hamming entre duas palavras-código distintas. Um QECC $\mathscr{C}$ com comprimento n, dimensão k, e distância mínima d é chamado código $[[n,k,d]]$. Um código com distância mínima d pode corrigir t erros ocorridos nos qubits de uma palavra-código, onde $t = \lfloor \frac{d-1}{2} \rfloor$. Em suma, QECC codificam k qubits em n qubits para proteger os dados se erros ocorrerem em quaisquer t desses n qubits, onde n,k e t são valores que dependem do código usado, [56].

Código corretor de erros bit flip

Suponha que qubits sejam enviados por um canal que os mantém inalterados com probabilidade $1-p$ e os inverte com probabilidade p. Ou seja, o estado $|\psi\rangle$ é levado para $X|\psi\rangle$ com probabilidade p, onde X é a matriz de Pauli conhecida também como operador *bit flip*. Esse canal é chamado canal *bit flip* ou de *inversão de bit*. O código *bit flip* que mostraremos agora protege qubits contra os efeitos de ruído deste canal.

Considere o estado de um qubit $\alpha|0\rangle + \beta|1\rangle$. Suponha que esse estado seja codificado com três qubits: $\alpha|000\rangle + \beta|111\rangle$. Podemos escrever essa operação de modo conveniente como

$$\begin{aligned} |0\rangle &\rightarrow |0_L\rangle \equiv |000\rangle \\ |1\rangle &\rightarrow |1_L\rangle \equiv |111\rangle, \end{aligned} \tag{3.2}$$

onde a notação $|0_L\rangle$ e $|1_L\rangle$ indica os estados lógicos $|0\rangle$ e $|1\rangle$ e não o "zero" e o "um" físicos. Assim, as superposições de estados da base são levadas nas superposições correspondentes nos estados codificados.

Suponha que o estado inicial $\alpha|0\rangle + \beta|1\rangle$ tenha sido perfeitamente codificado como $\alpha|000\rangle + \beta|111\rangle$. Cada um dos três bits é enviado através de uma cópia independente do canal *bit flip*. Ad-

mita que um erro tenha ocorrido em no máximo um qubit. Desejamos corrigir o erro sem perder a superposição $\alpha|000\rangle + \beta|111\rangle$. O procedimento de correção de erro para recuperar o estado original é dividido em dois estágios.

Primeiramente, devemos realizar uma medida sobre o estado quântico que irá detectar erro, caso haja algum. O resultado dessa medida é a *síndrome de erro*. Para o canal *bit flip* existem quatro síndromes de erro correspondentes aos seguintes operadores de projeção:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$$

Por exemplo, suponha que ocorreu um erro *bit flip* no primeiro qubit, ou seja, em vez do estado $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ o estado obtido após a transmissão é $|\psi'\rangle = \alpha|100\rangle + \beta|011\rangle$. A medida da síndrome é dada pelo operador $\langle\psi'|P_i|\psi'\rangle$, para $i = 0,1,2,3$. Nesse caso, temos

$$|\psi'\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \beta \\ \alpha \\ 0 \\ 0 \\ 0 \end{bmatrix}, \qquad \langle\psi'| = [0\ 0\ 0\ \beta\ \ \alpha\ 0\ 0\ 0],$$

e

$$P_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Logo,

$$\langle\psi'|P_1|\psi'\rangle = |\beta|^2 + |\alpha|^2 = 1.$$

Essa síndrome está associada ao erro no primeiro qubit. Se for feito o cálculo da síndrome, nesse caso, para os demais projetores, os resultados serão 0.

Enfatizamos que a medida da síndrome não altera o estado, pois a síndrome contém informação somente sobre qual erro ocorreu, mas não diz nada a respeito das amplitudes α e β. Ou seja, medindo a síndrome não estamos destruindo informação sobre o estado quântico em geral.

O segundo passo é utilizar o valor da síndrome para determinar qual o procedimento de recuperação do estado inicial. Por exemplo, se a síndrome de erro for 1, ou seja, se um erro ocorreu no primeiro qubit, então devemos inverter o qubit novamente aplicando o operador X, e assim obtemos exatamente o estado inicial $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$.

As possíveis síndromes de erro e seus correspondentes procedimentos de correção são dados na Tabela 3.4.

síndrome	**procedimento**
0	não faça nada
1	inverta o primeiro qubit
2	inverta o segundo qubit
3	inverta o terceiro qubit

Tabela 3.4: Síndromes de erros.

Esse procedimento de correção de erro funciona perfeitamente, se a inversão ocorrer em no máximo um dos três qubits. A probabilidade de que isso aconteça é $1-3p^2+2p^3$. Logo, a probabilidade de erro é $3p^2-2p^3$, exatamente como no caso clássico do código de repetição. Assim como no caso clássico, desde que $p < \frac{1}{2}$, a codificação e a decodificação aumentam a confiança na proteção do estado quântico.

Entretanto essa análise de erro não é completamente adequada. Com efeito, estados quânticos existem em um espaço contínuo, e pode acontecer de um erro corromper um estado de forma ínfima enquanto outros podem destruí-lo totalmente. Por exemplo, o operador X não afeta o estado $|+\rangle$, mas inverte os estados $|0\rangle$ e $|1\rangle$.

Isso pode dificultar o processo de recobrimento dos erros e, consequentemente sua correção. Porém, existe uma interpretação alternativa da medida de síndrome que faz uso do conceito de observável.

Definição 13 [56] *Uma medida projetiva é descrita por um observável M, que é um operador no espaço de estados do sistema sendo observado. O observável tem uma decomposição espectral*

$$M = \sum_m mP_m,$$

onde P_m é o projetor sobre o autoespaço de M com autovalor m. Os possíveis resultados da medida correspondem aos autovalores m do observável. Medindo-se o estado $|\psi\rangle$, a probabilidade de se

obter o resultado m é dada por

$$p(m) = \langle \psi | P_m | \psi \rangle.$$

Obtido o resultado m, o estado do sistema logo após a medida será

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

No modo alternativo de correção de erro *bit flip*, em vez de medirmos os projetores P_0, P_1, P_2 e P_3, executamos duas medidas, primeiro através do observável $Z_1Z_2 = Z \otimes Z \otimes I$ e, em seguida, do observável $Z_2Z_3 = I \otimes Z \otimes Z$. Cada um desses observáveis tem autovalores ± 1 e, portanto, cada medida fornece um único bit de informação em um total de dois bits de informação. A primeira medida de Z_1Z_2 compara o primeiro e o segundo qubits, para verificar se eles são iguais. Para ver isso, note que

$$Z_1Z_2 = (|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes I - |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I.$$

Se o resultado for $+1$, então os dois qubits são iguais, e se o resultado for -1 então, os dois qubits são diferentes. Analogamente, Z_2Z_3 compara os valores do segundo e terceiro qubits, resultando em $+1$ se eles forem iguais e -1 se forem diferentes. A partir dos resultados das duas medidas, determina-se se ocorreu um erro em algum qubit, e em caso positivo, em qual qubit. Na Tabela 3.5 listamos as possibilidades dessas medidas.

Autovalores de (Z_1Z_2, Z_2Z_3)	qubit onde ocorreu o erro
(+1,+1)	nenhum
(-1,+1)	primeiro qubit
(+1,-1)	terceiro qubit
(-1,-1)	segundo qubit

Tabela 3.5: Resultados das medidas de Z_1Z_2, Z_2Z_3.

Outros possíveis conjuntos de observavéis que podem ser usados para a medida das síndromes são: Z_1Z_3, Z_2Z_3 e Z_1Z_2, Z_1Z_3.

Algo importante a ser observado é que nenhuma medida nos fornece qualquer informação sobre as amplitudes α e β do estado quântico codificado, e, portanto, nenhuma medida destrói as superposições dos estados quânticos que desejamos preservar ao usarmos este código.

Detectado o erro, o passo seguinte é corrigi-lo. Obviamente, se nenhum erro ocorreu, nada se tem a fazer. Porém, se as síndromes indicarem que ocorreu um erro em algum qubit, devemos aplicar o operador X sobre o qubit onde esse erro ocorreu, e assim fazemos a correção.

Como no caso clássico do código de repetição de três bits, esse código tem distância $d = 3$ e é capaz de corrigir $t = 1$ erro.

Código corretor de erro phase flip

O código *bit flip* não apresenta inovação significativa sobre os códigos clássicos de correção. Veremos agora um canal ruidoso mais interessante conhecido como canal *phase flip* ou de inversão de fase para um qubit.

Esse canal preserva o qubit com probabilidade $1-p$, e inverte a fase dos estados $|0\rangle$ e $|1\rangle$ com probabilidade p. Ou seja, o operador *phase flip* Z, é aplicado ao qubit com probabilidade $p>0$, levando o estado $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ para $Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$. Ressaltamos que não existe equivalente clássico para esse canal. Contudo, existe uma forma simples de transformar o canal de inversão de fase em um canal de inversão de bit. Para isso, usaremos a base conjugada $\{|+\rangle, |-\rangle\}$. Nessa base, o operador Z troca $|+\rangle$ por $|-\rangle$ e vice-versa.

Os qubits lógicos são escritos na base conjugada como

$$\begin{aligned} |0_L\rangle &\equiv |{+}{+}{+}\rangle \\ |1_L\rangle &\equiv |{-}{-}{-}\rangle, \end{aligned}$$

onde

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

As operações de codificação, detecção de erro e recuperação são realizadas da mesma maneira que no caso do canal *bit flip*, porém em relação à base $\{|+\rangle, |-\rangle\}$. Esta mudança de base é obtida através da aplicação da porta de Hadamard sobre a base computacional $\{|0\rangle, |1\rangle\}$.

Para o processo de codificação, primeiro devemos codificar cada qubit de informação em três qubits, similarmente ao que foi feito para o caso bit flip. Em seguida, aplicamos a porta de Hadamard sobre cada um dos qubits.

A operação de codificação pode ser escrita na base computacional como:

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{1}{2\sqrt{2}}(|000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle - |111\rangle)$$

Apesar do código de repetição de três bits não aparecer explicitamente nessa operação, ele está presente na distribuição dos sinais antes de cada *ket*.

A detecção de um eventual erro é realizada aplicando-se as mesmas medidas projetivas do canal *bit flip*, porém conjugadas por portas de Hadamard: $P_i \rightarrow P_i' \equiv H^{\otimes 3} P_i H^{\otimes 3}$, onde $i = 0,1,2,3$. Equivalentemente, medidas de síndromes podem ser realizadas medindo-se os observáveis $X_1X_2 = H^{\otimes 3} Z_1 Z_2 H^{\otimes 3}$

e $X_2X_3 = H^{\otimes 3}Z_2Z_3H^{\otimes 3}$. A medida do observável X_1X_2 compara os sinais do primeiro e segundo qubits, enquanto a medida de X_2X_3 compara os sinais do segundo e terceiro qubits. Por exemplo, se temos estados como $|+\rangle|+\rangle \otimes (\cdot)$ ou $|-\rangle|-\rangle \otimes (\cdot)$, o resultado da medida de X_1X_2 é $+1$. Por outro lado, a medida desse observável resulta em -1 se temos estados do tipo $|+\rangle|-\rangle \otimes (\cdot)$ ou $|-\rangle|+\rangle \otimes (\cdot)$. Todas as possibilidades de resultados das medidas e os possíveis erros detectados são mostrados na Tabela 3.6.

Autovalores de (X_1X_2, X_2X_3)	bloco onde ocorreu o erro
(+1,+1)	nenhum
(-1,+1)	primeiro bloco
(+1,-1)	terceiro bloco
(-1,-1)	segundo bloco

Tabela 3.6: Resultados das medidas de X_1X_2, X_2X_3.

Outros conjuntos de observavéis poderiam ser utilizados: X_1X_3, X_2X_3 e X_1X_2, X_1X_3.

Para a correção de erros phase flip podemos aplicar os mesmos operadores usados no canal bit flip, porém conjugados pela matriz de Hadamard. Por exemplo, se foi detectada uma inversão no sinal em um qubit na posição i, basta aplicar o operador $Z = HXH$ sobre o qubit i para fazer a correção.

O código *phase flip* tem as mesmas características do código *bit flip*. Em particular, os critérios para o aumento da proteção, em comparação com o caso em que o código não é aplicado, são os mesmos. Além disso, esse código também tem distância $d = 3$ e corrige $t = 1$ erro.

O código de Shor $[[9,1,3]]$

Vimos que é possível construir um código que detecta e corrige erros *bit flip* e outro que detecta e corrige erros *phase flip*. Veremos agora um código que é capaz de corrigir um erro quântico arbitrário. O *código de Shor* com nove qubits, é uma combinação dos códigos de três qubits para os canais *bit flip* e *phase flip*.

Primeiramente, codificamos o qubit usando o código *phase flip*:

$$|0\rangle \to |+++\rangle$$

$$|1\rangle \to |---\rangle.$$

Em seguida, cada um desses qubits é codificado usando o canal *bit flip*:

$$|+\rangle \to \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$|-\rangle \rightarrow \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle).$$

O resultado é um código de nove qubits, com estados lógicos dados por:

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{1}{2\sqrt{2}}[(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)] \tag{3.3}$$

$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{1}{2\sqrt{2}}[(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)]. \tag{3.4}$$

O código de Shor não contradiz o teorema da não-clonagem, uma vez que uma palavra-código arbitrária é uma superposição dos dois estados lógicos.

Esse método de codificação usando níveis organizados hierarquicamente é conhecido como *concatenação*, e é uma maneira bastante útil de se obter códigos novos a partir de códigos conhecidos.

O código de Shor é capaz de proteger contra erros de inversão de bit e inversão de fase em qualquer qubit. Suponhamos, sem perda de generalidade, que um erro *bit flip* ocorreu no primeiro bloco de três qubits. Podemos detectá-lo através da medida dos observáveis Z_1Z_2 e Z_2Z_3, e corrigi-lo aplicando o operador X no qubit onde ocorreu o erro. Analogamente, se um erro desse tipo ocorrer no segundo ou terceiro blocos de qubits, podemos identificar o qubit corrompido fazendo a medida dos observáveis Z_4Z_5 e Z_5Z_6, Z_7Z_8 e Z_8Z_9, respectivamente. Em geral, não sabemos em que bloco exatamente o possível erro ocorreu, por isso é necessário realizar a medida desses seis observáveis.

Agora, considere que um erro *phase flip* ocorreu no primeiro qubit. Este erro troca a fase do primeiro bloco de três qubits. Observe que, seja qual for o qubit corrompido do bloco de três qubits, o efeito do erro é o mesmo. O observável $X_1X_2X_3X_4X_5X_6$ compara os sinais do primeiro e do segundo blocos de três qubits, e o observável $X_4X_5X_6X_7X_8X_9$ compara os sinais do segundo e do terceiro blocos também de três qubits, da mesma forma que no caso *bit flip* se comparava o sinal de dois qubits. Por exemplo, $(|000\rangle - |111\rangle)$ e $(000\rangle - |111\rangle)$ têm o mesmo sinal em ambos os blocos, enquanto $(|000\rangle - |111\rangle)$ e $(000\rangle + |111\rangle)$ têm sinais diferentes. De posse das medidas desses observáveis, é possível determinar em qual bloco de qubits ocorreu o erro de inversão de fase e depois corrigi-lo aplicando o operador Z sobre qualquer um dos qubits desse bloco.

Observe que, o fato dos erros do tipo Z provocarem o mesmo efeito em qualquer qubit de um bloco de três qubits no código de Shor está relacionado à propriedade de não-localidade, ou emaranhamento, pois o erro *phase flip* é identificado no bloco como um todo e não em cada qubit do bloco. Isso ocorre porque o qubit lógico não é codificado localmente. Por outro lado, o ruído é local, portanto isso aumenta a proteção contra o ruído.

Com esse código ainda é possível corrigir um erro *bit flip* e *phase flip* ocorrendo no mesmo qubit, ou seja, o operador ZX é aplicado a esse qubit corrompido. Basta aplicar os dois procedimentos

descritos acima. Note que, esses procedimentos são independentes. Porém, o código de Shor não corrige um erro de inversão de bit e um erro de inversão de fase se eles ocorrem em qubits diferentes. Ressaltamos que o código de Shor é melhor que os códigos clássicos de repetição no sentido de fazer uma busca por erros mais apurada. Na verdade, o código de Shor além de proteger contra inversões de bit e de fase sobre um qubit, ele também protege estados quânticos contra a ação de erros completamente arbitrários, desde que apenas um qubit seja afetado, [56]. Verifica-se que embora os erros possam ocorrer de forma contínua em um qubit, todos podem ser corrigidos corrigindo-se apenas um subconjunto discreto de erros; todos os outros erros possíveis ficarão automaticamente corrigidos. A discretização de erros é fundamental para explicar a eficácia das correções quânticas.

Destacamos os principais aspectos do código de Shor:

- Medir as síndromes não implica em medir os qubits. Os erros unitários X e Z podem ser invertidos sem que se conheça a informação codificada. Fazendo uma analogia com códigos clássicos, essa característica se assemelha ao processo de decodificação clássica quando a mensagem recebida do canal é projetada sobre uma classe lateral do arranjo padrão e a inversão do erro é feita pela palavra de peso mínimo.

- A codificação é não-local, enquanto os erros são locais. A informação é armazenada em vários qubits correlacionados, e os erros supõe-se que sejam locais. Assim, o $|0_L\rangle$ e o $|1_L\rangle$ são obtidos com probabilidade $\frac{1}{2}$ ao se medir um dos nove qubits do código de Shor. Se, eventualmente, o ambiente em volta do sistema "medir" um dos qubits, a informação codificada não será prejudicada, já que a informação não está contida totalmente em um qubit. Portanto, a informação codificada não é vulnerável a influências locais.

- O código de Shor pode corrigir um erro arbitrário ocorrido em um qubit.

- Erros do tipo Z têm o mesmo efeito em qubits diferentes dentro do mesmo bloco.

Baseado nas idéias do código de Shor pode-se construir códigos de correção de erro que podem corrigir erros em mais de um qubit.

3.4.3 Teoria quântica da correção de erro

Nesta seção mostramos como as idéias introduzidas pelo código de Shor podem ser naturalmente generalizadas para nos fornecer uma estrutura geral para o estudo da correção quântica de erro. São apresentadas as *condições para correção quântica de erro*. Uma estrutura que satisfaz tais condições nos fornece uma base que permite encontrar bons códigos de correção.

Em linhas gerais, estados quânticos são codificados por operações unitárias em um código quântico de correção que é definido como um subespaço $\mathscr{C}$ de algum espaço de Hilbert maior. O projetor sobre o espaço $\mathscr{C}$ será denotado por P. Após a codificação, ruído é adicionado no canal, em seguida é realizada a medida de síndrome para diagnosticar o tipo de erro que ocorreu. Uma vez que isso tenha sido determinado, uma operação de recuperação é realizada para retornar ao estado original. A idéia básica é que síndromes de erros diferentes correspondem a subespaços ortogonais e não-deformados do espaço de Hilbert. A razão desses subespaços serem ortogonais, é que do contrário, não poderiam ser distinguidos pela medida da síndrome. Além disso, os subespaços devem ser versões não-deformadas do espaço de codificação original, no sentido de que os processos de erro que mapeiam diferentes subespaços devem levar os estados codificados (ortogonais) a outros estados ortogonais a fim de que se possa corrigir o erro.

Faremos duas suposições gerais: o ruído é descrito por uma operação quântica ε, e o procedimento completo de correção de erro é efetuado por uma operação quântica $\mathscr{R}$ que preserva o traço, a qual é denominada *operação de correção de erro*. A operação $\mathscr{R}$ é responsável pela detecção e recuperação do erro. Para que a correção seja considerada bem sucedida, é necessário que, para qualquer estado ρ cujo suporte pertence ao subespaço do código $\mathscr{C}$ a seguinte equação seja satisfeita

$$(\mathscr{R} \circ \varepsilon)(\rho) \propto \rho.$$

O sinal $\propto$ é usado no lugar do sinal de igualdade porque algumas vezes pode ocorrer da operação ε não preservar o traço. Como a etapa de correção $\mathscr{R}$ deve ser bem-sucedida com probabilidade 1, exige-se que $\mathscr{R}$ preserve o traço.

As condições para correção quântica de erro formam um conjunto simples de equações que podem ser verificadas para determinar se um dado código de correção de fato protege o estado contra um tipo particular de ruído ε. Essas condições são utilizadas para construir uma grande quantidade de códigos, e ainda para investigar algumas propriedades gerais de códigos quânticos de correção de erros.

Teorema 5 [56] *Seja $\mathscr{C}$ um código quântico, e P um projetor sobre $\mathscr{C}$. Seja ε uma operação quântica com elementos de operação $\{E_a\}$. Uma condição necessária e suficiente para a existência de uma operação de correção de erro $\mathscr{R}$ corrigindo ε sobre $\mathscr{C}$ é que*

$$PE_a^\dagger E_b P = \alpha_{ab} P \tag{3.5}$$

para alguma matriz Hermitiana α de números complexos.

Os elementos de operação $\{E_a\}$ do ruído ε são chamados de erros, e se existir tal operação $\mathscr{R}$, diz-se que $\{E_a\}$ constitui um conjunto de erros corrigíveis.

Observamos no código de Shor que, sendo possível corrigir erros do tipo X e do tipo Z, então também é possível corrigir a combinação desses dois erros. O próximo teorema mostra que combinações lineares de erros corrigíveis também podem ser corrigidos pelas operações de correção $\mathscr{R}$.

Teorema 6 [56] *Seja $\mathscr{C}$ um código quântico e $\mathscr{R}$ a operação de correção de erro para recuperação de um processo de ruído ε com elementos de operação $\{E_a\}$. Seja $\mathscr{F}$ uma operação quântica com elementos de operação F_b que são combinações lineares dos elementos E_a, isto é, $F_b = \sum_a m_{ab} E_a$ para alguma matriz de números complexos m_{ba}. Resulta que a operação de correção de erro $\mathscr{R}$ também corrige os efeitos do processo de ruído $\mathscr{F}$ sobre o código $\mathscr{C}$.*

Em vez de falarmos de classes de processos de erros ε corrigíveis por um código $\mathscr{C}$ e operações de correção $\mathscr{R}$, podemos falar de *operadores de erro* (ou simplesmente *erros*) $\{E_a\}$ que são corrigíveis. Os teoremas acima implicam que, dados um código quântico $\mathscr{C}$ e operações de correção $\mathscr{R}$ que corrijam erros $\{E_a\}$, qualquer processo de ruído ε cujos elementos de operação sejam combinações lineares dos erros $\{E_a\}$ serão corrigidos também por $\mathscr{R}$.

Em suma, para combater o *continuum* de possíveis erros que podem ocorrer sobre um qubit é suficiente vencer a batalha contra um conjunto finito de erros, as quatro matrizes de Pauli, pois essas formam uma base para o espaço vetorial das matrizes 2×2. Heuristicamente, pode-se dizer que essas quatro matrizes são todos os possíveis erros que podem ocorrer em um qubit: nenhum erro (I), um erro *bit flip* (X), um erro *phase flip* (Z), e ambos os erros (Y). Para sistemas de dimensão mais alta usa-se como conjunto de erros, o grupo de Pauli de n qubits que será definido na próxima seção. Fazendo uma analogia com o caso clássico, a correção de erros para sistemas analógicos é extremamente difícil, porque, em princípio, existe um número infinito de diferentes síndromes de erros. Enquanto a correção digital de erros para o processamento de informação clássica envolve somente um número finito de síndromes de erro, o que a torna mais eficaz. Surpreendentemente, a correção quântica de erro é muito mais parecida com a correção digital clássica do que a correção analógica clássica, [56].

Códigos degenerados

Relembrando o efeito dos erros do tipo Z sobre as palavras-código do código de Shor, definimos uma classe de códigos quânticos bastante interessante chamada *códigos degenerados*, cuja propriedade fundamental é a impossibilidade de distinguir em que qubit ocorreu determinado erro, já que o efeito do erro é igual para diferentes qubits. Isso não ocorre nos códigos clássicos, pois erros em diferentes bits necessariamente implicam em diferentes palavras corrompidas. Essa característica dos códigos quânticos degenerados tem vantagem e desvantagem. Por um lado, algumas técnicas de demonstração

usadas classicamente em limites para correção de erros ficam invalidadas. Por exemplo, o limitante de Hamming que veremos a seguir. Por outro lado, esses códigos são capazes de "empacotar" mais informação do que os códigos clássicos, pois erros distintos não necessariamente levam o espaço do código para espaços ortogonais, e é possível, embora ainda não tenha sido provado, que essa capacidade extra permita que os códigos degenerados sejam capazes de armazenar a informação quântica de maneira mais eficaz do que os códigos não-degenerados.

Limitante quântico de Hamming

Como vimos no Capítulo 1, o limitante de Hamming é um critério para determinar se um dado código com certas características existe ou não, e se o limitante for satisfeito com igualdade o código então será perfeito. Infelizmente, o limitante quântico de Hamming é aplicável somente a códigos não-degenerados, mas ele aponta para algumas idéias de como devem ser os limites gerais. Suponha que um código não-degenerado seja usado para codificar k qubits em n qubits, de forma que ele possa corrigir erros em qualquer subconjunto com t ou menos qubits. Suponha que ocorram j erros, onde $j \leq t$. Ao todo existem $\left(\begin{array}{c} n \\ j \end{array} \right)$ possíveis conjuntos de posições onde o erro pode ocorrer. Para cada um desses conjuntos existem três tipos de erros possíveis, X, Y e Z, que podem ocorrer em cada qubit. Portanto, são ao todo, 3^j erros possíveis. Assim, o número total de erros que podem ocorrer em t ou menos qubits é:

$$\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right) 3^j$$

Note que $j = 0$ corresponde ao caso em que nenhum erro ocorre em qualquer um dos qubits; esse é o "erro" I. Para codificar k qubits de forma não-degenerada, cada um desses erros deve corresponder a um subespaço ortogonal com 2^k dimensões. Como todos esses subespaços devem estar contidos em um espaço de n qubits, com 2^n dimensões, então:

$$\sum_{j=0}^{t} \left(\begin{array}{c} n \\ j \end{array} \right) 3^j 2^k \leq 2^n \tag{3.6}$$

Essa desigualdade é chamada *limitante quântico de Hamming*.

Em particular, para $k = 1$ e $t = 1$, o limitante de Hamming torna-se:

$$2(1+3n) \leq 2^n$$

que só será satisfeita para $n \geq 5$. Portanto, um código não-degenerado para codificar um qubit contra qualquer tipo de erro não pode ter menos de cinco qubits. De fato, existe o código quântico de cinco qubits que atinge o limitante de Hamming.

Como nem todos os códigos quânticos são não-degenerados, o limitante quântico de Hamming é mais útil como uma regra prática para decidir sobre a existência de códigos quânticos. Até o momento não se conhece códigos que violem o limitante de Hamming, nem mesmo códigos degenerados.

Limitante quântico de Singleton

O limitante quântico de Singleton estabelece um limite para a capacidade dos códigos quânticos de correção de erro. Qualquer código quântico que codifique k qubits em n qubits, capaz de corrigir erros em quaisquer t qubits, deve satisfazer a relação

$$n \geq 4t + k. \tag{3.7}$$

Em particular, o menor código de um qubit capaz de corrigir erros arbitrários sobre um qubit satisfaz

$$n \geq 4 + 1 = 5.$$

Como $t = \lfloor \frac{d-1}{2} \rfloor$, então o limitante quântico de Singleton pode ser reescrito como

$$n - k \geq 2(d-1). \tag{3.8}$$

3.4.4 Códigos CSS

Um exemplo de uma ampla classe de códigos quânticos de correção de erros são os códigos CSS (Calderbank - Shor - Steane) que formam uma importante subclasse dos códigos estabilizadores que veremos na próxima seção.

Sejam C_1 e C_2 códigos clássicos lineares (n,k_1) e (n,k_2), tais que $C_2 \subset C_1$ e C_1 e $C_2^{\perp}$ corrigem ambos t erros. Considere $x \in C_1$, o estado quântico $|x+C_2\rangle$ é dado por:

$$|x+C_2\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x+y\rangle$$

onde a soma é realizada módulo 2. Seja x' um elemento de C_1 tal que $x - x' \in C_2$. Mostra-se que $|x+C_2\rangle = |x'+C_2\rangle$, e portanto o estado $|x+C_2\rangle$ depende somente da classe lateral C_1/C_2 a qual x pertence. Além disso, se x e x' pertencem a diferentes classes laterais de C_2, resulta que para nenhum $y, y' \in C_2$ ocorre $x+y = x'+y'$, e consequentemente $|x+C_2\rangle$ e $|x'+C_2\rangle$ são estados ortogonais. O código quântico CSS (C_1, C_2) é definido como o espaço vetorial gerado pelos estados $|x+C_2\rangle$ para todo $x \in C_1$. O número de classes laterais de C_2 em C_1 é $|C_1|/|C_2|$, logo a dimensão de CSS (C_1, C_2) é $|C_1|/|C_2| = 2^{k_1-k_2}$. Portanto, o código CSS (C_1, C_2) tem parâmetros $[[n, k_1 - k_2]]$.

Código de Steane

Destacamos agora um exemplo de um código CSS construído a partir do código de Hamming $(7,4,3)$, apresentado no exemplo 2.2.

Para simplificar, denotaremos o código de Hamming $(7,4,3)$ por C. Considere $C_1 \equiv C$ e $C_2 \equiv C^{\perp}$. Para que tenhamos um código CSS, é necessário que $C_2 \subset C_1$. Com efeito, por definição, a matriz verificação de paridade H de $C_2 \equiv C^{\perp}$ é igual à transposta da matriz geradora G de $C_1 \equiv C$:

$$H_{[C_2]} = G^T_{[C_1]} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Observe que, o espaço gerado pelas linhas de $H_{[C_2]}$ contém estritamente o espaço gerado pelas linhas de $H_{[C_1]}$ e, como os códigos são os núcleos de $H_{[C_2]}$ e $H_{[C_1]}$, conclui-se que $C_2 \subset C_1$. Além disso, $C_2^{\perp} \equiv (C^{\perp})^{\perp} \equiv C$, portanto C_1 e $C_2^{\perp}$ são códigos com distância 3, capaz de corrigir erros em um bit. Como C_1 é um código $(7,4)$ e C_2 um código $(7,3)$, conclui-se que CSS (C_1, C_2) é um código quântico $[[7,1]]$, capaz de corrigir erros em um único qubit, ou seja, um código $[[7,1,3]]$.

3.5 Códigos Estabilizadores

A teoria de correção quântica de erros apresentada na seção anterior fornece critérios para correção de erros, mas não fornece um método de construção de tais códigos. Veremos agora uma classe de códigos quânticos, desenvolvida por Gottesman, que compreende os códigos de Shor e CSS. Esses códigos, chamados *códigos estabilizadores*, têm sua construção baseada nos códigos lineares clássicos, no sentido de fazer uso de operadores que são analogias das matrizes verificação de paridade. Para isso, exploramos as propriedades de grupo fornecida pelo conjunto de operadores de Pauli. Para maiores informações sobre esse assunto sugerimos ao leitor as referências [18, 38, 39, 40, 41, 56, 62].

Para um único qubit, o grupo de Pauli consiste de todas as matrizes de Pauli junto com os fatores multiplicativos ± 1 e $\pm i$, ou seja, $\mathscr{G} = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$. Esse conjunto de matrizes forma um grupo, de ordem 16, sob a operação de multiplicação matricial. O grupo de Pauli geral, de n qubits, é definido como todas as matrizes formadas pelos produtos tensoriais de ordem n das matrizes de Pauli, com fatores multiplicativos ± 1 e $\pm i$.

Porém, podemos desconsiderar os valores imaginários desse grupo. Apesar de $\sigma_y \in \mathscr{G}_n$ ter componentes imaginárias, se σ_y aparecer um número par de vezes no produto tensorial, os coeficientes serão reais, e se σ_y aparecer um número ímpar de vezes os coeficientes nas palavras-código podem ser

imaginários. Contudo, Rains mostrou que sempre que um código complexo existir, existe também um código real com os mesmos parâmetros, [39].

Para contornar esse problema, alguns autores consideram

$$Y \equiv ZX \equiv i\sigma_y \equiv \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

onde $\sigma_y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, satisfazendo $Y^2 = -I$. Então os operadores $\pm I, \pm X, \pm Y, \pm Z = \pm\{I, X, Y, Z\}$ são os elementos de um grupo de ordem 8. Portanto, o grupo de Pauli de n qubits será o grupo $\mathscr{G} = \pm\{I,X,Y,Z\}^{\otimes n}$ de ordem 2^{2n+1}.

Os elementos do grupo de Pauli $\mathscr{G}_n$ satisfazem as seguintes propriedades:

- Cada $M \in \mathscr{G}_n$ é unitário, ou seja, $M^{-1} = M^\dagger$;
- Para cada $M \in \mathscr{G}_n$, temos $M^2 = \pm I \equiv \pm I^{\otimes n}$. Se o número de Y's no produto tensorial é par, então $M^2 = I$, e se o número de Y's no produto tensorial é ímpar, então $M^2 = -I$;
- Se $M^2 = I$, então M é Hermitiano ($M = M^\dagger$); se $M^2 = -I$, então M é anti-Hermitiano ($M = -M^\dagger$)
- Quaisquer dois elementos $M, N \in \mathscr{G}_n$ comutam ou anticomutam, $MN = \pm NM$.

O grupo de Pauli é usado para caracterizar os QECC. Considere o espaço de Hilbert $\mathscr{H}$ com 2^n dimensões e o grupo de Pauli de n qubits $\mathscr{G}_n$. Denote por S um subgrupo abeliano do grupo de Pauli de n qubits $\mathscr{G}_n$. Assim todos os elementos de S agindo em $\mathscr{H}$ podem ser simultaneamente diagonalizados. Define-se o *código estabilizador* $\mathscr{C}_S \subseteq \mathscr{H}$ associado a S como o autoespaço simultâneo com autovalor 1 de todos os elementos de S. Ou seja,

$$C = \{|\psi\rangle; M|\psi\rangle = |\psi\rangle \quad \forall M \in S\}.$$

O grupo S é chamado *estabilizador* do código, uma vez que preserva todas as palavras-código, e seus elementos são chamados *operadores estabilizadores*. Estados quânticos, e portanto, códigos quânticos, são descritos de forma mais compacta através dos operadores que o estabilizam.

Não é qualquer subgrupo S de $\mathscr{G}_n$ que pode ser utilizado como estabilizador para um espaço vetorial não-trivial. Duas condições devem ser satisfeitas por S, são elas: os elementos de S devem comutar, e $-I$ não pode ser um elemento de S. De fato, suponha que o vetor não-nulo $|\psi\rangle \in \mathscr{C}_S$, e sejam $M, N \in S$. Então, M e N são produtos tensoriais das matrizes de Pauli, possivelmente com um fator de fase global multiplicativo. Como as matrizes de Pauli comutam ou anticomutam entre si, segue que M e N devem comutar ou anticomutar. Para verificar a primeira condição vamos supor que M e N anticomutam.

Por hipótese, $-NM = MN$, e portanto $-|\psi\rangle = -NM|\psi\rangle = MN|\psi\rangle = |\psi\rangle$, ou seja $|\psi\rangle = 0$. Para estabelecer a segunda condição, note que, se $-I \in S$, então $-I|\psi\rangle = |\psi\rangle$, ou seja, $|\psi\rangle = 0$.

O grupo S pode ser descrito de maneira mais compacta através de seus geradores. Um conjunto de elementos independentes de S, $\{M_1,\ldots,M_l\}$, gera S se todo elemento de S pode ser escrito como um produto dos elementos $M_1,\ldots,M_l$. Dessa maneira, o grupo S pode ser caracterizado por seus geradores $\{M_i\}$. Assim, para ver se um vetor em particular é estabilizado por S, é preciso apenas verificar se o vetor é estabilizado por seus geradores.

Afirmação 1 *Se S tem $n-k$ geradores, então o espaço do código $\mathscr{C}_S$ tem dimensão 2^k, ou seja, $\mathscr{C}_S$ codifica k qubits.*

Demonstração: Com efeito, sejam $\{M_1,M_2,\ldots,M_{n-k}\}$ os geradores de S. Como vimos, para cada $M \in S$ tem-se $M^2 = I$, do contrário M teria autovalor diferente de $+1$. Para cada $M \neq \pm I$ existe pelo menos um $N \in \mathscr{G}_n$ tal que N anticomuta com M. Daí, os autovalores $+1$ e -1 ocorrem com probabilidades iguais. Começamos a nossa demonstração considerando $M = M_1$. Temos que $M_1|\psi\rangle = |\psi\rangle$ se, e somente se, $M_1N|\psi\rangle = -NM_1|\psi\rangle = -N|\psi\rangle$. Isto é, N estabiliza autoestados associados aos autovalores $+1$ e autoestados associados aos autovalores -1 de M_1 com probabilidades iguais. Portanto, temos $\frac{1}{2}(2^n) = 2^{n-1}$ estados mutuamente ortogonais tais que $M_1|\psi\rangle = |\psi\rangle$.

Agora, seja $M_2 \in \mathscr{G}_n$ tal que $M_2 \neq \pm I, \pm M_1$ e comuta com M_1. Existe um $N \in \mathscr{G}_n$ que comuta com M_1 e anticomuta com M_2. Assim, N preserva o autoespaço associado ao autovalor $+1$ de M_1 e, dentro desse espaço, altera na mesma proporção os autoestados associados aos autovalores $+1$ e -1 de M_2. Logo, o espaço satisfazendo

$$M_1|\psi\rangle = M_2|\psi\rangle = |\psi\rangle.$$

tem dimensão 2^{n-2}.

Seguindo esse processo, seja $M_j \in \mathscr{G}_n$ independente de $\{M_1,M_2,\ldots,M_{j-1}\}$ e que comuta com todo $M_i, i = 1,\ldots,j-1$, então existe um N que comuta com $M_1,M_2,\ldots,M_{j-1}$ e anticomuta com M_j. Portanto, no espaço $M_1 = M_2 = \ldots = M_{j-1}$, M_j tem tanto autovetores associados ao autovalor $+1$ quanto autovetores associados aos autovalores -1. Cada vez que adicionamos um gerador, a dimensão dos autoespaços simultâneos é dividida ao meio. Então, com $n-k$ geradores, a dimensão do espaço é $(\frac{1}{2})^{n-k}2^n = 2^k$. ∎

Os $n-k$ geradores do estabilizador S funcionam como os *operadores verificação de paridade* de um código. Ou seja, são os observáveis que medimos para diagnosticar os erros. Por exemplo, digamos que uma informação foi codificada. Se $M_i = 1$ para todo i, $(i = 1,2,\ldots,n-k)$, então não é

detectado nenhum erro. Porém, se $M_i = -1$ para algum i, então o estado da informação está contido em um autoespaço ortogonal ao subespaço do código, consequentemente um erro será detectado.

Seja $\varepsilon = \{E_a\} \subset \mathscr{G}_n$ o conjunto de erros que desejamos corrigir. Um operador erro E_a pode ser escrito em termos dos elementos do grupo de Pauli. Em particular, E_a comuta ou anticomuta com um gerador particular M do estabilizador S. Se E_a comuta com M temos,

$$ME_a|\psi\rangle = E_aM|\psi\rangle = E_a|\psi\rangle,$$

para $|\psi\rangle \in \mathscr{C}_S$. Logo, o erro E_a preserva o valor $M = 1$. Porém, se E_a anticomuta com M temos,

$$ME_a|\psi\rangle = -E_aM|\psi\rangle = -E_a|\psi\rangle.$$

Ou seja, o erro troca o valor de M, e pode ser detectado através de uma medida de M.

Em alguns casos é útil definir a *síndrome de erro para um código estabilizador*. Para geradores estabilizadores M_i e erros E_a, seja $f_M : \mathscr{G}_n \to \mathbb{Z}_2$ dada por

$$f_M(E_a) = \begin{cases} 0, & \text{se} \quad [M,E_a] = 0 \\ 1, & \text{se} \quad \{M,E_a\} = 0 \end{cases}$$

e $f(E_a) = (f_{M_1}(E_a), \ldots, f_{M_{n-k}}(E_a))$. Então $f(E_a)$ é uma sequência binária de $(n-k)$-bits. Para fazer a operação de correção de erro para um código estabilizador, devemos medir os autovalores dos geradores do estabilizador. O autovalor de cada M_i é $(-1)^{f_{M_i}(E_a)}$, que nos dará a síndrome de erro. Se o código é não-degenerado, então os $f_{M_i}(E_a)$ serão distintos para todo $E_a \in \varepsilon$ e medindo os $n-k$ geradores é possível diagnosticar o erro completamente, ou seja, cada erro tem uma síndrome diferente, de modo que a síndrome indica exatamente o erro que ocorreu. Porém, se o código é degenerado, então existem erros distintos com síndromes iguais, e portanto, as síndromes apontam qual conjunto de erros degenerados ocorreu.

Mais geralmente, existe uma condição a ser satisfeita pelo estabilizador que é suficiente para que um erro seja detectado e corrigido. Uma variação do Teorema 5 diz que dado ε espaço de erros agindo em um espaço de Hilbert $\mathscr{H}$, então um subespaço $\mathscr{C}$ de $\mathscr{H}$ é um QECC corrigindo os erros ε se, e somente se, para todo $E_a, E_b \in \varepsilon$ e $|\psi\rangle \in \mathscr{C}$ normalizado, temos que

$$\langle\psi|E_a^\dagger E_b|\psi\rangle = \alpha_{ab},$$

onde α_{ab} é independente de $|\psi\rangle$, [40]. Isso é verdade se uma das seguintes condições for satisfeita:

1. $E_a^\dagger E_b \in S$.

2. Existe um $M \in S$ que anticomuta com $E = E_a^\dagger E_b$.

Com efeito, se o item 1 ocorrer então, $\langle\psi|E_a^\dagger E_b|\psi\rangle = \langle\psi|\psi\rangle = 1$ para $|\psi\rangle \in \mathscr{C}_S$. E se o item 2 ocorrer, então $\langle\psi|E_a^\dagger E_b|\psi\rangle = \langle\psi|E_a^\dagger E_b M|\psi\rangle = -\langle\psi|ME_a^\dagger E_b|\psi\rangle = -\langle\psi|E_a^\dagger E_b|\psi\rangle$, portanto $\langle\psi|E_a^\dagger E_b|\psi\rangle = 0$, [62].

Assim, um código estabilizador que corrige o conjunto de erros $\{\varepsilon\}$ é um espaço $\mathscr{C}_S$ fixado por um subgrupo abeliano S do grupo de Pauli $\mathscr{G}_n$, onde (1) ou (2) é satisfeito por cada $E_a^\dagger E_b$ com $E_a, E_b \in \varepsilon$. O código é não-degenerado se a condição (1) não é satisfeita para qualquer $E_a^\dagger E_b$.

O subgrupo abeliano S com $n-k$ geradores define 2^{n-k} autoespaços simultâneos. Qualquer um desses autoespaços pode ser escolhido como espaço de codificação. Cada um desses autoespaços gera um código, e todos esses códigos são equivalentes no sentido de que diferem somente no rotulamento dos qubits e na escolha da base utilizada para a descrição dos mesmos. Portanto, o estabilizador de um código pode ser transformado no estabilizador de outro código por permutação dos qubits junto com um produto tensorial de transformações de um qubit.

Como o estabilizador S é um subgrupo abeliano de $\mathscr{G}_n$, os operadores de $\mathscr{G}_n$ que não comutam com todos os $M_i \in S$ mapeiam $\mathscr{C}_S$ em seu complemento ortogonal, consequentemente são erros detectáveis. Entretanto, existem muitos elementos de $\mathscr{G}_n$ que comutam com todo $M \in S$ mas não pertencem a S. Operadores com esta característica preservam o subespaço de codificação $\mathscr{C}_S$, mas não agem trivialmente sobre ele, podendo corromper a informação. Por exemplo, suponha que $E_a^\dagger E_b$ comuta com todo elemento do estabilizador mas não está nele. Como $E_a|\psi\rangle$ e $E_b|\psi\rangle$ têm a mesma síndrome, podemos interpretar erroneamente um erro E_a como um erro E_b; o efeito do erro junto com a tentativa em corrigi-lo nos faz aplicar $E_b^\dagger E_a$ ao dado, o que pode causar dano.

O *peso* de um operador de Pauli é o número de fatores no tensor que difere de I. Um código estabilizador com distância d tem a propriedade que cada $E \in \mathscr{G}_n$ com peso menor que d, pertence ao estabilizador ou anticomuta com algum elemento dele. Sob esse aspecto, se o estabilizador não contém elementos de peso menor que d, então o código é não-degenerado. Para que um código corrija t erros, sua distância deve ser pelo menos $d = 2t+1$, e um código com distância $s+1$ pode detectar s erros ou corrigir s erros em locais conhecidos, [62].

Uma outra maneira de caracterizar os códigos estabilizadores é utilizando conceitos de teoria de grupos como centralizador e normalizador. Podemos definir o conjunto de elementos de $\mathscr{G}_n$ que comutam com todos os elementos de S como o *centralizador* $C(S)$ de S em G_n. Devido às propriedades de S e $\mathscr{G}_n$, pode-se mostrar que o centralizador é igual ao *normalizador* $N(S)$ de S em $\mathscr{G}_n$, onde o normalizador é definido como o conjunto de elementos de $\mathscr{G}_n$ que fixam S sob conjugação. De fato,

para quaisquer $A \in \mathscr{G}_n$ e $M \in S$, temos

$$A^\dagger MA = \pm A^\dagger AM = \pm M.$$

Como $-I \notin S$, segue que

$$A \in N(S) \Leftrightarrow A \in C(S),$$

donde, $N(S) = C(S)$, [39].

Observe que, $S \subseteq N(S)$. Se $E \in N(S) - S$, então para $M \in S$ e $|\psi\rangle \in \mathscr{C}_S$, temos

$$ME|\psi\rangle = EM|\psi\rangle = E|\psi\rangle,$$

logo $E|\psi\rangle \in \mathscr{C}_S$. Como $E \notin S$, existe algum estado em $\mathscr{C}_S$ que não é fixado por E. Temos que E difere de um elemento de S por uma fase total, e portanto não será um erro detectável por esse código.

Assim, podemos afirmar que um código quântico com estabilizador S detecta todos os erros E que pertencem a S ou anticomutam com algum elemento de S.

A distância de um código quântico é d se, e somente se, $N(S) - S$ não contém elementos de peso menor que d. Dizemos que o código é degenerado se S tem elementos diferentes da identidade de peso menor que d. Caso contrário, dizemos que o código é não-degenerado.

O código de Shor revisitado

Do ponto de vista de estabilizadores, o código *bit flip* de três qubits é um código quântico $[[3,1,3]]$ onde o estabilizador é $S = \langle Z_1Z_2, Z_2, Z_3\rangle$ e as palavras-código $|0_L\rangle$ e $|1_L\rangle$ são autovetores com autovalores $+1$ dos geradores Z_1Z_2 e Z_2, Z_3, [56].

Observe que todo produto tensorial de dois elementos do conjunto de erros $\varepsilon = \{I, X_1, X_2, X_3\}$ anticomuta com pelo menos um dos geradores de S (exceto para a identidade). Logo, ε é um conjunto corrigível para esse código.

Como vimos, a detecção de erros é feita através da medida dos geradores de S. Por exemplo, se ocorreu um erro X_1 então os autovalores de Z_1Z_2 e Z_2Z_3 são -1 e $+1$, respectivamente. Se o erro X_2 ocorreu, temos que os resultados da medida da síndrome são -1 e -1. Se ocorreu o erro X_3, então temos como resultados $+1$ e -1. Obviamente, I nos fornece como resultados $+1$ e $+1$. Em cada um desses casos, a correção é feita aplicando-se a operação inversa ao erro indicado.

Similarmente, podemos ver o código phase flip sob o aspecto de códigos estabilizadores. Temos que o estabilizador é $S = \langle X_1X_2, X_2X_3\rangle$, e o conjunto de erros corrigíveis é $\varepsilon = \{I, Z_1, Z_2, Z_3\}$. Além disso, as relações $M_i|u_L\rangle = |u_L\rangle$ e $\bar{Z}|u_L\rangle = (-1)^u|u_L\rangle$, onde $u = 0,1$ e $i = 1,2$, são satisfeitas para as palavras-código $|0_L\rangle$ e $|1_L\rangle$.

Agora vejamos o código de Shor em termos do formalismo estabilizador. O código de Shor é um código quântico estabilizador $[[9,1,3]]$ cujo estabilizador S tem oito geradores, veja a Tabela 3.7.

Nome	Operador
M_1	$Z\,Z\,I\,I\,I\,I\,I\,I\,I$
M_2	$I\,Z\,Z\,I\,I\,I\,I\,I\,I$
M_3	$I\,I\,I\,Z\,Z\,I\,I\,I\,I$
M_4	$I\,I\,I\,I\,Z\,Z\,I\,I\,I$
M_5	$I\,I\,I\,I\,I\,I\,Z\,Z\,I$
M_6	$I\,I\,I\,I\,I\,I\,I\,Z\,Z$
M_7	$X\,X\,X\,X\,X\,X\,I\,I\,I$
M_8	$I\,I\,I\,X\,X\,X\,X\,X\,X$
$\overline{Z}$	$X\,X\,X\,X\,X\,X\,X\,X\,X$
$\overline{X}$	$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$

Tabela 3.7: Geradores e operações lógicas do código de Shor.

Como vimos na Seção 3.4.2, o código de Shor corrige todos os tipos de erros de um qubit. Isso pode ser comprovado para todos os operadores de Pauli com peso menor ou igual a dois. Ou seja, esse código tem distância três. Por exemplo, digamos que ocorreram erros de um qubit X_1 e Y_4. O produto X_1Y_4 anticomuta com Z_1Z_2, logo não pertence ao normalizador $N(S)$. Da mesma maneira verifica-se que todos os produtos de dois erros do conjunto de erros ou pertencem a S ou anticomutam com pelo menos um elemento de S. Segue que o código de Shor pode corrigir um erro arbitrário em um qubit.

Podemos ver que as palavras-código $|0_L\rangle$ e $|1_L\rangle$ em (3.3) e (3.4), são autovetores com autovalores $+1$ de todos os geradores M_i, $i = 1,\ldots,8$. Além disso, cada operador de $\mathscr{G}_n$ que fixa $|0_L\rangle$ e $|1_L\rangle$ pode ser escrito como produto dos geradores M_i's. O grupo formado por esses operadores é o grupo estabilizador S.

O código CSS e o código $[[7,1,3]]$ **revisitados**

Sejam C_1 e C_2 códigos clássicos lineares (n,k_1) e (n,k_2) tais que $C_2 \subset C_1$ e ambos, C_1 e $C_2^{\perp}$, corrigem t erros. Defina uma matriz verificadora com a forma

$$\begin{bmatrix} H_{C_2^{\perp}} & 0 \\ 0 & H_{C_1} \end{bmatrix}$$

Essa matriz verificadora corresponde ao estabilizador do código CSS (C_1,C_2), [56].

Para ver que isso define um código estabilizador, é necessário que a matriz verificadora satisfaça a condição de comutatividade $H_{C_2^{\perp}}H_{C_1}^T = 0$. Devido a $C_2 \subset C_1$, temos que $H_{C_2^{\perp}}H_{C_1}^T = [H_{C_1}G_{C_2}]^T = 0$. De fato, pode-se verificar que esse é exatamente um código CSS (C_1,C_2), e que ele é capaz de corrigir erros arbitrários em t qubits.

O código de sete qubits de Steane é um exemplo de código CSS, cuja matriz verificadora de paridade é

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

A codificação dos operadores Z e X para o código de Steane é definida por:

$$\overline{Z} \equiv Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7; \qquad \overline{X} \equiv X_1 X_2 X_3 X_4 X_5 X_6 X_7.$$

O código de cinco qubits

O tamanho mínimo de um código quântico que codifica um único qubit de forma que qualquer erro no seu estado codificado possa ser detectado e corrigido é cinco. O código $[[5,1,3]]$ satura o limitante quântico de Hamming e, portanto, é um código quântico perfeito. Os geradores do estabilizador e as operações lógicas Z e X do código de cinco qubits são mostrados na Tabela 3.8.

Nome	Operador
M_1	$X\,Z\,Z\,X\,I$
M_2	$I\,X\,Z\,Z\,X$
M_3	$X\,I\,X\,Z\,Z$
M_4	$Z\,X\,I\,X\,Z$
$\overline{Z}$	$Z\,Z\,Z\,Z\,Z$
$\overline{X}$	$X\,X\,X\,X\,X$

Tabela 3.8: Geradores e operações lógicas para o código $[[5,1,3]]$.

Capítulo 4

Códigos Quânticos Topológicos

O computador quântico pode ser bastante promissor, porém a decoerência resultante das interações entre o sistema e o ambiente que o cerca e os erros sistemáticos em transformações unitárias são problemas que dificultam a construção de tais computadores. Para construir um computador quântico é necessário que a informação quântica seja protegida durante o processo de computação, isso é o que chamamos de *computação tolerante à falhas*. Por exemplo, a correção quântica de erros, introduzida por Shor é uma forma de realizar computação quântica tolerante à falhas.

Existem muitas idéias para a construção de um computador quântico, uma dessas é a *computação quântica topológica*, que propõe usar certas propriedades de partículas confinadas em um plano. Pode parecer uma teoria estranha, mas essas propriedades já foram observadas na prática em uma área denominada *física do efeito Hall quântico*. Atualmente, outros experimentos estão sendo propostos e executados na esperança de se obter uma computação quântica topológica rudimentar.

Para evitar as interações entre o sistema e o ambiente circundante, o caminho mais natural seria isolar os qubits de suas vizinhanças, porém ao se considerar um número grande de qubits esse passa a ser um desafio muito difícil. A computação quântica topológica propõe um caminho alternativo onde estados quânticos dependem de propriedades topológicas de um sistema físico. Assim, deformações contínuas causadas pelo ambiente não seriam capazes de alterar tais propriedades, e então teríamos naturalmente uma computação quântica tolerante à falhas.

Essa computação é realizada por meio de "cordas" entrançadas que representam o movimento da partícula no espaço-tempo. As partículas envolvidas nesse processo não são de um tipo comum, elas possuem certas propriedades matemáticas especiais e são conhecidas como *anyons*, cujo nome nada tem a ver com os "ânions" (íons de carga negativa). A idéia de usar tais partículas para realizar computação quântica tolerante à falhas partiu originalmente do físico Alexei Yu Kitaev em 1997, [48]. Entretanto, a possibilidade de usar topologia para esse propósito foi considerada antes por Michael H.

Freedman em 1988, e publicada apenas em 1998.

Iniciamos esse capítulo apresentando o código tórico de Kitaev na Seção 4.1. Na Seção 4.2 mostramos como pode se realizar computação quântica tolerante à falhas através de anyons. A Seção 4.3 mostra outros códigos quânticos topológicos em superfícies com gênero $g = 0$ e $g = 1$, baseados nas idéias de Kitaev.

4.1 Código Tórico

Os códigos tóricos descritos inicialmente por Kitaev, associam qubits às arestas de um reticulado quadrado de um toro. Esses códigos podem ser generalizados para uma classe mais ampla, os *códigos quânticos topológicos* (ou simplesmente TQC), considerando outras superfícies orientáveis bidimensionais diferentes do toro. Os códigos TQC formam uma subclasse dos códigos estabilizadores.

Intuitivamente, um reticulado no $\mathbb{R}^n$ é um conjunto infinito de pontos dispostos de forma regular. Formalmente, um reticulado Λ é definido como um subconjunto discreto infinito de $\mathbb{R}^n$ que forma um grupo aditivo sob adição usual de vetores. Aqui iremos considerar o reticulado quadrado gerado pelos vetores $\mathbf{u} = (1,0)$ e $\mathbf{v} = (0,1)$. Um toro é uma superfície orientável com gênero um, ou seja, é equivalente a uma esfera com uma "alça". Nas Seções 5.1.1 e 6.2 aprofundaremos os conceitos de reticulado e toro. Um toro planar pode ser descrito como um quadrado cujos lados opostos são identificados. Então, entenda um reticulado quadrado no toro como um ladrilhamento por quadrados unitários no toro planar ($\mathbb{Z} \times \mathbb{Z}$), como mostrado na Figura 4.1.

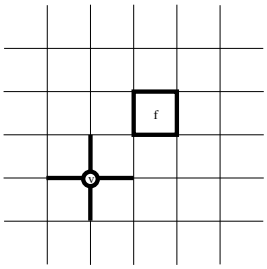

Figura 4.1: Reticulado quadrado do toro.

Considere um reticulado quadrado $l \times l$ no toro. Sejam V, E e F o conjunto dos vértices, arestas e faces do reticulado, respectivamente. Os qubits estão em correspondência um-a-um com as arestas do reticulado. Como cada aresta pertence simultaneamente a duas faces do reticulado, temos que $|E| = 2l^2$, ou seja, o comprimento do código é $n = |E| = 2l^2$ qubits.

Os operadores estabilizadores, por sua vez, estão associados aos vértices e às faces do reticulado. Dado um vértice $v \in V$ o operador vértice A_v é definido como o produto tensorial de σ_x correspondendo

a cada uma das quatro arestas que tem v como vértice comum e o operador identidade agindo nos qubits restantes. Analogamente, dada uma face $f \in F$, o operador face B_f é definido como o produto tensorial σ_z correspondendo a cada uma das quatro arestas que formam o bordo da face f e o operador identidade agindo nos demais qubits. Ou seja,

$$A_v = \bigotimes_{j \in E} \sigma_x^{\delta(j \in E_v)} \qquad B_f = \bigotimes_{j \in E} \sigma_z^{\delta(j \in E_f)}, \tag{4.1}$$

onde δ é o delta de Kronecker.

Esses operadores são de fato operadores estabilizadores. Cada A_v e B_f é Hermitiano e tem autovalores ± 1. Além disso, operadores vértice A_v obviamente comutam uns com os outros assim como operadores face B_f. Apesar de σ_x e σ_z anticomutarem, como operadores face e operadores vértice possuem duas ou nenhuma aresta em comum, segue que A_v e B_f comutam.

Portanto, o código tórico é o subespaço $\mathscr{C}$ do espaço de Hilbert $\mathscr{H}$ com $2^n = 2^{2l^2}$ dimensões, que é fixado pelos operadores A_v e B_f:

$$\mathscr{C} = \{|\psi\rangle : A_v|\psi\rangle = |\psi\rangle,\ B_f|\psi\rangle = |\psi\rangle \ \ \forall\ v, f\} \tag{4.2}$$

Observe que

$$\prod_v A_v = 1 \quad \text{e} \quad \prod_f B_f = 1. \tag{4.3}$$

Assim, um operador vértice pode ser escrito como um produto dos demais operadores vértice, assim como um operador face também pode ser escrito como um produto dos demais operadores face. Logo, existem $2l^2 - 2$ geradores do estabilizador S formado pelos operadores A_v e B_f. Como vimos na Seção 3.5, se S tem $n-2$ geradores, então a dimensão do código é $2^2 = 4$, ou seja, $\mathscr{C}$ codifica $k = 2$ qubits. O número de qubits codificados está relacionado com o número de ciclos fundamentais da superfície, [63, 31], no caso do toro temos dois ciclos, o paralelo e o meridiano, e por isso $k = 2$. Ou ainda, o número de qubits codificados é igual a $2g$, e como o gênero do toro é 1, então $k = 2$.

Antes de definir a distância de um código tórico, temos que introduzir alguns conceitos de teoria de homologia, [7, 34]. Uma *1-cadeia* é uma aplicação que fixa um elemento de $\mathbb{Z}_2$ a cada aresta do reticulado. Em um abuso de linguagem, usaremos também o termo para nos referir ao conjunto de todas as arestas que são fixadas ao valor 1 por essa aplicação. Analogamente, uma *0-cadeia* e uma *2-cadeia* são definidas como as aplicações correspondentes que fixam um elemento de $\mathbb{Z}_2$ aos vértices e às faces do reticulado, respectivamente. Assim, uma 1-cadeia forma um espaço vetorial sobre $\mathbb{Z}_2$, onde a soma de duas cadeias é, intuitivamente, uma união das arestas contidas nas duas 1-cadeias. Da mesma forma, 0-cadeia e 2-cadeia também formam espaços vetoriais.

O operador linear *bordo* ∂ pode ser definido de uma 1-cadeia à uma 0-cadeia, e de uma 2-cadeia à uma 1-cadeia. Sejam v_0, v_1, v_2 os vértices de uma face triangular, o *bordo* de uma aresta $\partial(v_0, v_1)$ é a 0-cadeia $v_1 - v_0$, e o bordo de uma face $\partial(v_0, v_1, v_2)$ é a 1-cadeia $\partial(v_0, v_1) + \partial(v_1, v_2) + \partial(v_2, v_0)$, considerando a orientação da face. Define-se um *ciclo* como uma cadeia cujo bordo é trivial. Um ciclo é dito *homologicamente trivial* se pode ser escrito como o bordo de uma 2-cadeia. Do contrário, o ciclo é chamado *homologicamente não-trivial*.

Lembramos que um operador de Pauli que não comuta com os operadores estabilizadores é um erro detectável, enquanto que um operador de Pauli que comuta com todos os operadores estabilizadores preserva o subespaço codificador. Por outro lado, um operador que comuta com o estabilizador mas não pertence a ele pode corromper a informação. Assim, a distância de um código estabilizador é o peso do operador de Pauli de menor peso que preserva o subespaço codificador e não age trivialmente nele. Vejamos isso em termos de ciclos.

Qualquer operador de Pauli pode ser expresso como um produto tensorial de X's (e I's) vezes um produto tensorial de Z's (e I's). O produto de Z's e I's define uma 1-cadeia, onde arestas cujo operador Z age correspondem ao valor 1 e arestas cujo operador I age correspondem ao valor 0. O operador definido por esse produto trivialmente comuta com todos os operadores face, e comuta com um operador vértice se, e somente se, um número par de Z's agem nas arestas adjacentes ao vértice. Portanto, essa 1-cadeia é na verdade um ciclo. Similarmente, o produto tensorial de X's e I's trivialmente comuta com os operadores vértice, e comuta com um operador face se, somente se um número par de X's agem nas arestas contidas na face. As arestas no reticulado dual nas quais X age formam um ciclo do reticulado dual.

Assim, um operador de Pauli que comuta com o estabilizador do código pode ser representado como um produto tensorial de operadores Z agindo em um ciclo do reticulado, vezes um produto tensorial de operadores X agindo em um ciclo do reticulado dual.

Em um reticulado, o interior de um ciclo homologicamente trivial pode ser "ladrilhado" por faces da tesselação, e assim um produto tensorial de operadores Z agindo nas arestas deste ciclo pode ser escrito como um produto de operadores faces que o compõe, e portanto está contido no estabilizador. Como vimos, esse tipo de operador age trivialmente sobre o código. O mesmo acontece com o operador formado por produtos tensoriais de X agindo num ciclo homologicamente trivial no reticulado dual.

Em geral, qualquer elemento do estabilizador pode ser escrito como um produto tensorial de operadores Z agindo em um ciclo homologicamente trivial do reticulado vezes um produto tensorial de operadores X agindo em um ciclo homologicamente trivial do reticulado dual. Conclui-se que o

espaço gerado pelos operadores que agem em ciclos homologicamente triviais é identificado com o estabilizador.

Por outro lado, se um produto de operadores Z corresponde a um ciclo homologicamente não-trivial, então este operador ainda comuta com o estabilizador porém, não está contido nele. Logo a distância do código tórico é o peso do operador correspondente a um ciclo homologicamente não-trivial, de menor peso. Ou seja, a distância mínima de $\mathscr{C}$ é o mínimo entre o número de arestas contidas no menor ciclo homologicamente não-trivial do reticulado e o número de arestas contidas no menor ciclo homologicamente não-trivial do reticulado dual. Lembrando que o reticulado quadrado $l \times l$ é auto-dual, ou seja, esse número de arestas é igual para o reticulado e o reticulado dual, segue que o menor desses caminhos corresponde aos eixos ortogonais do reticulado ou do reticulado dual (Figura 4.2), portanto $d = l$, [22].

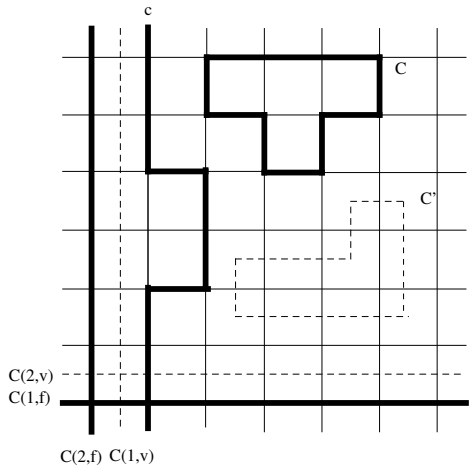

Figura 4.2: Os ciclos C e C' são homologicamente triviais no reticulado e no reticulado dual, respectivamente. Os demais ciclos são homologicamente não-triviais no reticulado e no reticulado dual.

Realiza-se a correção de um erro aplicando o operador de Pauli de peso mínimo.

Em qualquer sistema quântico local com diferença de massa, existe um *estado base* que é o estado onde não existem partículas. No plano o estado base é único, porém em uma superfície bidimensional com topologia não-trivial, o estado base é degenerado, e o grau de degeneração depende da topologia, [63].

No caso do toro, considere os dois ciclos fundamentais que denotaremos por C_1 e C_2, e defina operadores unitários T_1 e T_2 que descrevem o processo de criação de um par de partículas (*anyon* e *anti-anyon*), onde o *anyon* se propaga em c_1 e c_2, respectivamente, antes do par se aniquilar. Assim, T_1 e T_2 preservam o estado base do sistema, pois ambos comutam com o Hamiltoniano H que descreve o sistema, e portanto, podem ser simultaneamente diagonalizados. Contudo, T_1 e T_2 não comutam

um com o outro, logo não podem ser simultaneamente diagonalizados. Para ver isso, considere o comutador de T_1 e T_2

$$T_2^{-1}T_1^{-1}T_2T_1 = e^{-i2\theta}I,$$

onde $e^{i\theta}$ é a fase de permutação de *anyon* (veja Seção 4.2.2). Note que, o caminho descrito por $T_2^{-1}T_1^{-1}T_2T_1$ é equivalente a um processo no qual um *anyon* dá uma volta em torno de outro no sentido horário. Uma volta no sentido horário equivale a duas permutações sucessivas no sentido horário, representada pela fase $e^{-i2\theta}$. Portanto, T_1 e T_2 não comutam, exceto para $\theta = 0$ e $\theta = \pi$.

Como T_1 é unitário, então seus autovalores são fases. Seja $\alpha \in [0, 2\pi)$ um autoestado de T_1 com autovalor $e^{i\alpha}$. Assim, $T_1|\alpha\rangle = e^{i\alpha}|\alpha\rangle$. Aplicando T_2 ao autoestado de T_1 temos,

$$T_1(T_2|\alpha\rangle) = e^{i2\theta}T_2T_1|\alpha\rangle = e^{i2\theta}e^{i\alpha}(T_2|\alpha\rangle).$$

Suponha que θ seja um múltiplo rotacional de 2π, ou seja, $\theta = \pi\frac{p}{q}$, onde p e q são inteiros positivos primos entre si ($p < 2q$). Então T_1 deve ter pelo menos q autovalores distintos. T_1 agindo em α gera uma órbita com q valores distintos. Como T_1 comuta com o Hamiltoniano, no toro o estado base do sistema anyônico deve ter grau de degeneração igual a um múltiplo de q. Verifica-se que o grau da degeneração é exatamente q, [63]. Em uma superfície de gênero g, existem operadores análogos a T_1 e T_2 associados a cada uma das g "alças", então o grau de degeneração topológica torna-se q^g.

No modelo de Kitaev, será mostrado na Seção 4.2.3 que existem dois tipos de partículas, então existem dois tipos de operadores T_1, digamos $T_{1,v}$ e $T_{1,f}$, e dois tipos de operadores T_2, $T_{2,v}$ e $T_{2,f}$. Os comutadores são $T_{2,f}^{-1}T_{1,v}^{-1}T_{2,f}T_{1,v} = -1 = T_{2,v}^{-1}T_{1,f}^{-1}T_{2,v}T_{1,f}$. Assim, $T_{1,v}$ e $T_{2,v}$ podem ser simultaneamente diagonalizados e interpretados como os operadores lógicos $\overline{Z_1} = \bigotimes_{j\in E}\sigma_z^{\delta(j\in C_{1,f})}$ e $\overline{Z_2} = \bigotimes_{j\in E}\sigma_z^{\delta(j\in C_{2,f})}$. O operador $T_{2,f}$ que comuta com $\overline{Z_1}$ e anticomuta com $\overline{Z_2}$, pode ser visto como o operador lógico $\overline{X_1} = \bigotimes_{j\in E}\sigma_x^{\delta(j\in C_{1,v})}$. Analogamente, o operador $T_{1,f}$ pode ser visto como o operador lógico $\overline{X_2} = \bigotimes_{j\in E}\sigma_x^{\delta(j\in C_{2,v})}$, veja os ciclos na Figura 4.2. O Hamiltoniano no modelo de Kitaev é

$$H_0 = -\sum_v A_v - \sum_f B_f. \tag{4.4}$$

E o grau de degeneração é 4. O estado base de H_0 coincide com o subespaço protegido do código. Todos os estados excitados são separados por uma diferença de energia $\Delta E \geq 2$, devido a diferença entre os autovalores dos operadores estabilizadores ser igual a dois.

Os operadores que compõem o Hamiltoniano H_0 são locais. Medir um desses operadores requer uma computação quântica, mas devido ao fato de cada um desses operadores envolver poucos qubits (4 qubits) no bloco do código, e desses qubits estarem próximos uns dos outros, a medida pode ser

executada realizando poucas portas quânticas. Isso facilita a potencial implementação física desses sistemas reticulados. Ao contrário dos códigos topológicos, os operadores estabilizadores em códigos não-topológicos são geralmente não-locais.

Com essas características Kitaev consegue mostrar que, apesar desses códigos não serem bons códigos no sentido de não atingirem o limitante de Hamming, eles proporcionam algumas vantagens diante de problemas como decoerência (veja Seção 4.2.3). A probabilidade de erro tende a zero na mesma proporção que $exp(-al)$.

Essa construção não é restrita a reticulados quadrados. Além disso, pode-se considerar um reticulado em uma superfície bidimensional qualquer. Para superfícies de gênero g, $2g$ qubits podem ser codificados, pois a cada "alça" adicionada, existem dois novos ciclos de homologia, e daí, existem dois novos $\overline{Z}$'s lógicos.

4.2 Computação Quântica Topológica

Uma das principais aplicações da correção quântica de erros é a computação quântica tolerante à falhas, ou seja, a proteção da informação quântica durante o processo dinâmico da computação. A computação quântica tolerante à falhas permite manter inalterado um estado quântico por um tempo suficiente para completar um cálculo computacional, desde que a taxa de erro seja constante. Essa taxa de erro é a probabilidade de decoerência de um qubit codificado por unidade de tempo. Veremos nesta seção que é possível implementar a computação de forma arbitrariamente boa, mesmo com portas lógicas defeituosas, desde que a probabilidade de erro por porta esteja abaixo de um determinado limiar constante, [56].

A computação clássica também pode ser feita tolerante à falhas, porém desnecessária devido a suas portas lógicas serem suficientemente seguras para isso. A informação clássica é armazenada em um meio magnético, que provém de spins de átomos individuais, onde cada spin é bastante sensível à flutuações térmicas. Os spins interagem uns com os outros e tendem a ser orientados na mesma direção. Se algum spin se move na direção oposta, as forças de interação movem-no de volta para a direção dos demais. Pode-se dizer que erros estão sendo corrigidos no nível físico, [48]. Surge a dúvida se algo semelhante seria possível fazer no caso quântico.

A partir disso, Kitaev propõe uma computação quântica tolerante à falhas baseada em propriedades de partículas conhecidas como *anyons* que só são possíveis em um mundo bidimensional. O hardware nesse modelo terá uma resistência natural a falhas.

Nesta seção veremos os aspectos gerais da computação quântica resistente à falhas, as propriedades

particulares dos *anyons* que permitem tal computação, e a maneira como é realizada a computação através de *anyons*.

4.2.1 Aspectos gerais de tolerância à falhas

A idéia central da computação quântica tolerante à falhas é computar diretamente com estados quânticos codificados, de tal forma que a decodificação não seja necessária. Suponha que seja dado um circuito simples. O ruído atua em cada um dos elementos que compõem esse circuito: na preparação do estado, nas portas lógicas quânticas, na medida na saída, e até mesmo na transmissão da informação ao longo dos fios. Para combater os efeitos do ruído, cada qubit do circuito original é substituído por um bloco de qubits codificados, usando um QECC. Além disso, cada porta do circuito original é substituída por uma rotina que implementa uma porta codificada, que por sua vez atua no estado codificado. Uma maneira de evitar o acúmulo de erros é realizar correções de erro periodicamente no estado codificado. Mas só isso não é suficiente, pois as portas codificadas podem causar a propagação de erros, e as correções de erro em si podem introduzir erros nos qubits codificados. Para evitar isso, as portas codificadas devem ser cuidadosamente projetadas, de modo que uma falha qualquer durante o procedimento para sua codificação se propague somente em um número pequeno de qubits em cada bloco de qubits codificados, permitindo que o procedimento de correção seja eficaz. Esses procedimentos para codificar portas são chamados *resistentes à falhas*. De modo semelhante, deve-se ter cuidado no projeto do procedimento de correção para não introduzir muitos erros nos dados.

Além de portas quânticas codificadas, a computação quântica também precisa de procedimentos de medida e de preparação de estados tolerantes a falhas. Sabemos que as medidas são usadas para codificar, ler os resultados da computação, diagnosticar a síndrome nas correções, e preparar estados auxiliares para a construção de portas, e portanto, as medidas são cruciais para a computação quântica tolerante à falhas. Um procedimento para medir um observável em um conjunto de qubits codificados é resistente à falhas se uma falha de um único componente do procedimento resultar no máximo em um erro em um qubit em cada bloco de qubits na saída do procedimento. Além disso, exige-se que, se somente um componente falhar, o resultado da medida deve ter probabilidade de erro $O(p^2)$, onde p é a probabilidade de falha em qualquer um dos componentes. Esse último requisito é extremamente importante, pois o resultado da medida pode ser usado para controlar outras operações no computador quântico e, se ela estiver incorreta, o erro pode se propagar, afetando muitos qubits em outros blocos de qubits codificados. Diz-se que um procedimento para preparar um estado codificado é tolerante à falhas se uma falha em um único componente do procedimento resultar no máximo em um erro em um qubit em cada bloco de qubits ao final do procedimento.

Portanto, a resistência a falhas de um certo procedimento é a propriedade de que, se apenas uma componente do procedimento falhar, ocorrerá apenas um erro em cada bloco de qubits codificados na saída, [56].

É possível implementar eficientemente a computação quântica em escala arbitrária desde que o ruído em portas quânticas individuais esteja abaixo de um certo limiar constante.

Teorema 7 (Teorema do Limiar)[56] *Um circuito quântico contendo $p(n)$ portas pode ser simulado com probabilidade de erro de no máximo ε usando*

$$O(poli(\log p(n)/\varepsilon)p(n))$$

portas no seu hardware, com probabilidade de falha de cada componente no máximo igual a p, desde que p seja menor que um limiar $p < p_{lm}$, e supondo-se condições razoáveis para o ruído no hardware.

Uma estimativa superficial para esse limiar é $p_{lm} \approx 10^{-4}$, contudo, cálculos mais sofisticados fornecem valores na faixa $10^{-5} - 10^{-6}$, [56].

A idéia é realizar operações resistentes a falhas diretamente sobre os estados codificados, intercalando com etapas de correção de erros, levando a uma redução na probabilidade de ocorrência de erro de p para $O(p^2)$.

Uma maneira de reduzir ainda mais essa probabilidade é concatenar códigos várias vezes e criar procedimentos resistentes à falhas hierárquicos. O teorema do limiar não afirma a possibilidade de proteger a computação quântica contra os efeitos de ruído totalmente arbitrário. As hipóteses fisicamente razoáveis a que o teorema se refere são sobre o tipo de ruído que ocorre em um computador quântico, e uma arquitetura computacional disponível para permitir que o seu resultado se aplique.

4.2.2 Anyons

Vimos na Seção 3.2 que para partículas idênticas no espaço de três dimensões, comum na física, a permutação dessas partículas são representadas de duas maneiras. Se as partículas são bósons, então uma permutação entre duas partículas é representada pelo operador identidade agindo na função de onda, ou seja, a função de onda é invariante, e dizemos que a partícula obedece as estatísticas de Bose. Se as partículas são férmions, então uma permutação dessas é representada pela multiplicação por (-1), ou seja, a função de onda troca o sinal, e dizemos que a partícula obedece as estatísticas de Fermi. Estatística de um sistema é a propriedade que descreve como o vetor estado do sistema se transforma sob a troca de duas partículas, [63].

A estatística de partículas idênticas em uma, três ou mais dimensões, é um conceito bem estabelecido. Já para duas dimensões, uma variedade consideravelmente rica de tipos de estatísticas de partículas é possível. A permutação de partículas idênticas, neste caso, pode mudar a função de onda por uma multiplicação de fase $e^{i\theta}$ que toma outros valores além de 1 e -1. Ou seja, o fator de multiplicação pode se tornar um número complexo qualquer.

Da mesma forma que ocorria com o fator de fase -1, a multiplicação da função de onda por um fator complexo não tem efeito sobre as propriedades mensuráveis da partícula individual. A fase pode alterar o modo pelo qual duas ondas complexas interferem.

Partículas indistinguíveis em duas dimensões não são bósons nem férmions, são o que se conhece como "quasipartículas" e se comportam de maneira muito semelhante à das partículas e antipartículas da física de altas energias. Essas quasipartículas são conhecidas por *anyons*, e esse nome se deve ao fato do fator de multiplicação poder ser "qualquer" (any) número complexo.

Pode-se pensar que *anyons* sejam apenas uma construção teórica, mas eles também são realizações físicas de sistemas reais que podem ser estudadas em laboratórios. Alguns experimentos recentes indicam que os *anyons* existem em certas estruturas semicondutoras planares especiais, resfriadas até perto do zero absoluto e imersas em campos magnéticos intensos. Um *gás bidimensional de elétrons* pode existir na interface de duas placas semicondutoras de arseneto de gálio. Os elétrons se movem livremente nas duas dimensões da interface, mas são impedidos de se mover na direção ortogonal à camada, que os tiraria do plano. Em um campo magnético suficientemente forte e em temperatura extremamente baixa, e se os elétrons no material são suficientemente móveis, o gás bidimensional de elétrons atinge um estado base profundamente emaranhado que é separado de todos os estados excitados por um intervalo de energia diferente de zero, [63]. Por exemplo, no caso do *efeito Hall quântico fracionário* as excitações no gás de elétrons se comportam como partículas dotadas de apenas uma fração da carga do elétron. Outras excitações carregam unidades de fluxo magnético consigo, como se o fluxo fosse parte integrante de sua estrutura, [19]. Uma confirmação experimental de que as quasipartículas do estado Hall quântico fracionário são *anyons* foi obtida por Vladimir J. Goldman, Fernando E. Camino e Wei Zhou em 2005.

A razão de *anyons* existirem somente em duas dimensões é que em um mundo tridimensional existe a propriedade topológica que diz que um caminho fechado nesse espaço pode ser suavemente contraído a um ponto. Portanto, a fase topológica $e^{i\theta}$ adquirida pela função de onda quando duas quasipartículas são permutadas é 1 ou -1, pois $\theta = 0$ ou $\theta = \pi$. Já em duas dimensões, não existe essa propriedade, logo qualquer valor de θ é possível em princípio, [63]. Esta característica está relacionada com o conceito físico conhecido como *efeito Ahoronov - Bohm*.

Em duas dimensões, é necessário saber em que direção ocorre a permutação de duas partículas: se elas seguem percursos horários ou anti-horários. Os dois percursos alternativos são topologicamente distintos, pois não é possível deformar continuamente um percurso horário em um anti-horário sem cruzar trajetos e as partículas envolvidas colidirem. Assim, a fase adquirida pela função de onda depende dessa propriedade.

Anyons podem ser de dois tipos: abelianos e não-abelianos. Por exemplo, suponhamos que haja três *anyons* enfileirados, ocupando as posições A, B, C. Primeiramente, permutemos os *anyons* localizados nas posições A e B. Em seguida, troquemos os *anyons* em B e C. O resultado é uma função de onda modificada por algum fator de fase. Suponhamos agora que primeiro se permutem os *anyons* em B e C, e depois em A e B. Se a função de onda resultante tem o mesmo fator de fase que a anterior, os *anyons* são denominados abelianos. Se os fatores dependem da ordem em que se realizam as permutações, eles são não-abelianos. Para a construção de um computador quântico topológico pesquisadores acreditam que se deve usar *anyons* não-abelianos, [54]. Esta propriedade significa que a ordem em que as partículas são permutadas é importante, e decorre do fato de que, para *anyons* desse tipo, o fator que modifica a função de onda é uma matriz de números, e o resultado da multiplicação de matrizes depende da ordem em que elas são colocadas.

4.2.3 Computação anyônica

Kitaev mostra que um sistema quântico bidimensional com excitações anyônicas pode ser considerado um computador quântico. As transformações unitárias são obtidas através de *cordas* entrançadas conhecidas como *linhas do universo*, que representam os movimentos dessas excitações uma em volta da outra. Tal computação é tolerante à falhas por sua natureza física.

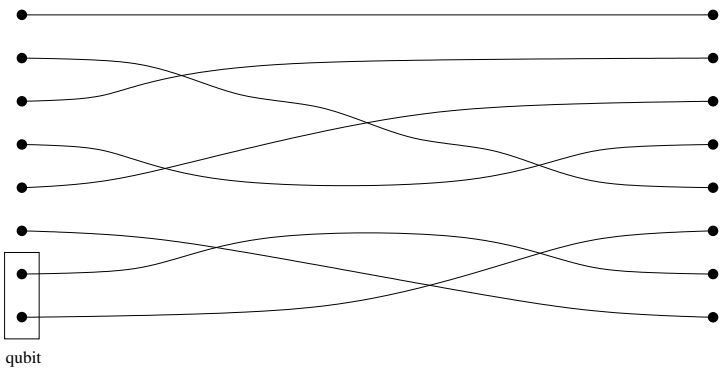

Figura 4.3: Movimento de anyons no espaço-tempo.

Uma computação quântica poderia ser realizada da seguinte maneira: primeiro criam-se pares de

anyons enfileirados, cada par se parece bastante com uma partícula e sua antipartícula correspondente, ambas nascidas de energia pura. Em seguida, os pares de *anyons* são movimentados um em volta do outro, em uma sequência cuidadosamente determinada. A linha do universo de cada *anyon* é como um fio, e o movimento dos *anyons*, conforme eles são permutados, entrança os fios (Figura 4.3). A computação quântica é codificada nesse entrançamento, que contém o estado final dos *anyons*, [19]. A medida pode ser feita unindo as excitações em pares e observando o resultado de suas fusões.

Em seguida explicaremos cada uma das etapas dessa computação:

1. Criação de pares de *anyons*;
2. Evolução (transformações unitárias);
3. Medida.

Criação de pares de *anyons*

É impossível criar uma única partícula. Contudo, é possível criar um par de partículas da seguinte forma

$$|\psi^z(t)\rangle = S^z(t)|\xi\rangle \qquad |\psi^x(t')\rangle = S^x(t')|\xi\rangle,$$

onde $|\xi\rangle$ é um estado base qualquer, e

$$S^z(t) = \bigotimes_{j\in E} \sigma_z^{\delta(j\in t)} \qquad S^x(t') = \bigotimes_{j\in E} \sigma_x^{\delta(j\in t')}.$$

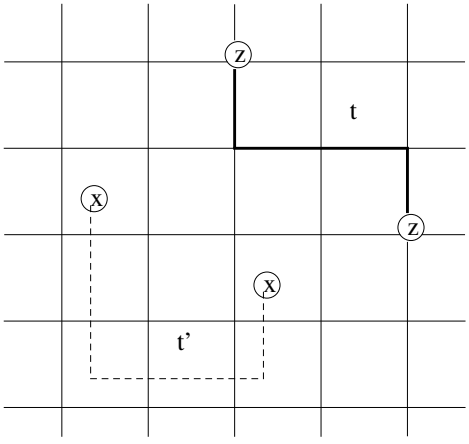

Figura 4.4: Cordas e partículas.

No caso de $|\psi^z(t)\rangle = S^z(t)|\xi\rangle$, são criadas duas partículas nos pontos finais da corda t, veja Figura 4.4. Tais partículas encontram-se nos vértices do reticulado, e são chamadas *partículas do tipo-z*

ou *cargas elétricas*, porque carregam carga elétrica. No segundo caso, são geradas duas partículas nas extremidades da corda t', ou seja, essas partículas estão nas faces do reticulado e são chamadas *partículas do tipo-x* ou *fluxos magnéticos*, porque carregam fluxo magnético. Os operadores $S^z(t)$ e $S^x(t')$ são chamados *operadores corda*. Note que, esses operadores comutam com todo operador A_v e B_f, exceto com aqueles que correspondem às extremidades da corda. O estado $|\psi^z(t)\rangle$ depende apenas da classe de homotopia do caminho t, enquanto o operador $S^z(t)|\xi\rangle$ depende de t.

Qualquer configuração de um número par de partículas do tipo-z e um número par de partículas do tipo-x pode ser realizada. Podemos conectar o par de partículas por cordas em um caminho qualquer. Cada uma dessas configurações define um subespaço 4^g-dimensional no espaço de Hilbert $\mathscr{H}$. Esse subespaço é independente das cordas, porém um vetor particular $S^{a_1}(t_1)\ldots S^{a_m}(t_m)|\xi\rangle$ depende de $t_1,\ldots,t_m$. Portanto, se desenharmos essas cordas em um caminho topologicamente diferente obtemos outro vetor no mesmo subespaço de 4^g dimensões.

Se uma partícula do tipo-x se move em torno de uma partícula do tipo-z (no sentido anti-horário), começando e terminando no mesmo ponto (veja Figura 4.5), então seu estado inicial

$$|\psi_{inicial}\rangle = S^z(t)|\psi^x(q)\rangle$$

torna-se

$$|\psi_{final}\rangle = S^x(c)S^z(t)|\psi^x(q)\rangle = -S^z(t)S^x(c)|\psi^x(q)\rangle = -S^z(t)|\psi^x(q)\rangle = -|\psi_{inicial}\rangle,$$

pois $S^x(c)$ e $S^z(t)$ anticomutam e $S^x(c)|\psi^x(q)\rangle = |\psi^x(q)\rangle$. Portanto, a função de onda total adquire um fator de fase -1. Isso não ocorre se as partículas são do mesmo tipo. Como já foi mencionado, a ação não-trivial do operador descrito acima causa um efeito que só é possível ocorrer em sistemas bidimensionais (efeito Ahoronov-Bohm).

Assim, dada uma partícula, podemos saber de que tipo ela é fazendo com que *anyons* de teste sejam movidos em volta desta partícula e observando se houve troca de fase.

Evolução

Como foi mencionado no início deste capítulo, Michael H. Freedman já havia considerado a possibilidade de usar a topologia para computação quântica. Suas idéias baseavam-se na relação entre "invariantes de nós" e física quântica de uma superfície bidimensional evoluindo no tempo. A possibilidade de criar um sistema físico desse tipo, e de se realizar uma medida adequada sobre ele, fará com que o invariante de nó seja computado aproximadamente, de maneira automática, em vez de se fazer um cálculo longo e inconveniente em um computador convencional.

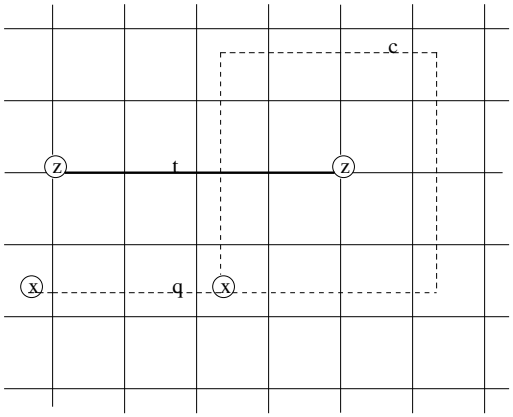

Figura 4.5: Uma partícula tipo-x movendo-se em torno de uma partícula tipo-z.

Vimos que a permutação das partículas entrançam suas linhas do universo e existe uma ação não-trivial no vetor estado da partícula. Existe uma interpretação topológica desses entrançamentos relacionada a *teoria dos nós*. Mais especificamente, essa é uma representação física do chamado *grupo de braid* ou *grupo de tranças*. O estado quântico de n partículas pertence a um espaço de Hilbert que evolui como uma representação unitária do grupo de *braid* B_n. Essa estrutura matemática descreve todas as maneiras como uma dada fileira de fios pode ser entrançada. Qualquer entrançamento pode ser produzido a partir de uma série de operações elementares em que dois fios adjacentes são movimentados, seja no sentido horário, seja no anti-horário.

Suponha que n partículas ocupam n posições ordenadas $1,2,\ldots,n$ arranjadas em uma linha. Denote por σ_1 uma permutação no sentido anti-horário das partículas que inicialmente ocupavam as posições 1 e 2, denote por σ_2 uma permutação no sentido anti-horário das partículas cujas posições iniciais eram 2 e 3, e assim por diante. Qualquer *trança* ou *braid* pode ser construído com uma sucessão de permutações de partículas vizinhas, ou seja, $\sigma_1,\sigma_2,\ldots,\sigma_{n-1}$ são os geradores do grupo de *braid* B_n, desde que satisfaçam as seguintes relações:

1. $\sigma_i\sigma_j = \sigma_j\sigma_i$ se $|i-j| \geq 2$

2. $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$.

Essas relações estão representadas na Figura 4.6. A primeira relação significa que permutações de pares disjuntos de partículas comutam. A segunda relação é conhecida como *equação de Yang-Baxter*, e também podemos escrevê-la como

$$(R\otimes I)(I\otimes R)(R\otimes I) = (I\otimes R)(R\otimes I)(I\otimes R), \tag{4.5}$$

onde R é uma matriz e I é a matriz identidade com a mesma ordem de R, veja Figura 4.7. Na Figura 4.6 pode-se observar que ambos $\sigma_1\sigma_2\sigma_1$ e $\sigma_2\sigma_1\sigma_2$ descrevem um processo no qual as partículas nas posições 1 e 3 são permutadas no sentido anti-horário sobre a partícula 2, que permanece fixa, portanto esses *braids* são topologicamente equivalentes.

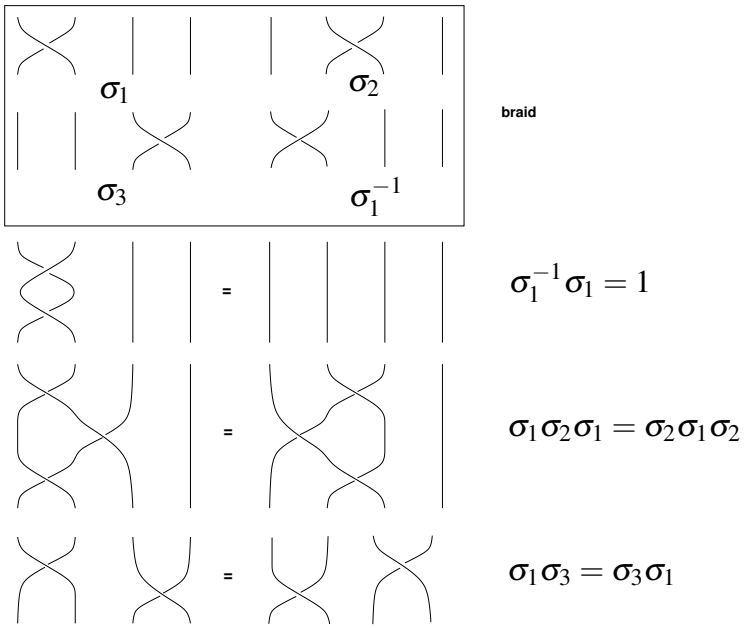

Figura 4.6: Geradores de tranças e relações.

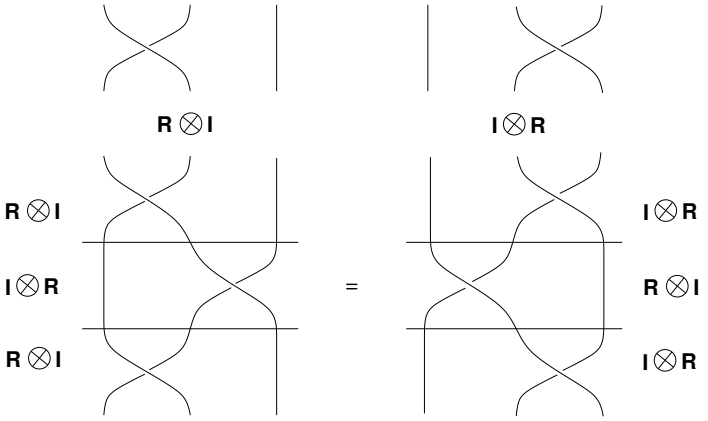

Figura 4.7: Equação de Yang-Baxter.

Um entrançamento é uma aplicação linear associada a cada cruzamento elementar, e é conhecido como *operador braiding*. Também pode ser visto como uma matriz, chamada matriz *braiding*. Uma solução unitária R para a equação de Yang-Baxter pode ser vista topologicamente como uma matriz braiding ou quanticamente como uma porta universal, [47]. Toda sequência possível de manipulações

de *anyons* corresponde a um entrançamento, e vice-versa. Por sua vez, cada entrançamento corresponde a uma matriz que resulta da combinação de todas as matrizes que representam as permutas de *anyons*, [19].

Como o grupo de *braid* é infinito, tem-se um número infinito de representações unitárias irredutíveis, e de fato existe uma quantidade infinita de representações unidimensionais. Os *anyons* abelianos são as partículas indistinguíveis que evoluem como uma representação unidimensional do grupo de *braid*. Com efeito, nas representações unidimensionais, cada gerador σ_j de B_n é representado por uma fase $\sigma_j = e^{i\theta_j}$. Portanto a relação de Yang-Baxter torna-se $e^{i\theta_j}e^{i\theta_{j+1}}e^{i\theta_j} = e^{i\theta_{j+1}}e^{i\theta_j}e^{i\theta_{j+1}}$, o que implica que $e^{i\theta_j} = e^{i\theta_{j+1}} \equiv e^{i\theta}$, ou seja, todas as permutações são representadas pela mesma fase. Por outro lado, no grupo de *braid* também existem representações não-abelianas que são de dimensão maior que 1. As partículas indistinguíveis que se transformam como tais representações são os *anyons* não-abelianos. Para obter uma computação quântica tolerante à falhas deve-se operar *anyons* não-abelianos, [63, 48].

Medida

Para obter a leitura do resultado da computação, devemos medir os estados dos *anyons*. Se eles estiverem muito distantes, a medição é impossível. Então, eles precisam ser aproximados aos pares. Grosso modo, verifica-se se os pares se aniquilam perfeitamente, como deve ocorrer com antipartículas verdadeiras, ou se eles deixam resíduos de carga e fluxo, o que revela como seus estados foram alterados pelo entrançamento a partir da situação exata de antipartículas que iniciaram.

Enfatizamos que um computador quântico de *anyon* e um computador quântico convencional têm potência computacional equivalente, segundo um teorema provado por M. Freedman, A. Kitaev e Z. Wang, [30].

Erros em uma computação quântica topológica podem ocorrer se flutuações térmicas produzirem um par extra de *anyons* enroscados no entrançamento da computação antes de se aniquilarem mutuamente. Entretanto, a probabilidade de ocorrência dessa interferência diminui exponencialmente conforme aumenta a distância percorrida pelos *anyons*. A taxa de erros pode ser minimizada mantendo-os suficientemente distantes. Além disso, o processo de geração térmica é suprimido nas baixas temperaturas em que um computador topológico poderia operar. Assim, pode-se alcançar qualquer precisão desejada com a construção de um computador suficientemente grande, mantendo os *anyons* bem afastados no entrançamento, [19].

Entretanto, a computação quântica topológica ainda está no início. Ainda não se demonstrou a existência dos *anyons* não-abelianos, e a mais simples das portas lógicas ainda está sendo construída.

Se for mostrado que *anyons* não-abelianos de fato existem, então computadores quântico topológicos terão a chance de superar os projetos mais convencionais na corrida para ir de qubits e portas lógicas até máquinas completas, pois a probabilidade de erro cai exponencialmente conforme a temperatura é baixada e a escala de tamanho cresce. Esse fator exponencial é a principal contribuição da topologia, e não tem nenhum análogo nas abordagens mais tradicionais da computação quântica.

4.3 Outros Códigos Quânticos Topológicos em Superfícies com Gênero $g = 0$ e $g = 1$

De uma maneira geral, pode-se utilizar a construção de Kitaev em outras superfícies bidimensionais para obtenção de códigos quânticos topológicos corretores de erros. Apresentamos nessa seção códigos quânticos topológicos construídos no plano projetivo $\mathbb{R}P^2$ e códigos tóricos sob uma nova interpretação dos códigos de Kitaev.

4.3.1 Códigos sobre o plano projetivo

A partir da construção de Kitaev, M. Freedman e D. Meyer, em [31], construíram códigos sobre o plano projetivo $\mathbb{R}P^2$. Nesse trabalho eles mostram quatro códigos distintos, um com parâmetros $[[15,1,3]]$, e três com parâmetros $[[9,1,3]]$, dentre os quais um é equivalente ao código de Shor de nove qubits.

Como no plano projetivo existe apenas um ciclo fundamental, segue que $k = 1$. O comprimento do código é dado pelo número de arestas ($n = |E|$), assim como no código de Kitaev, e a distância é o número de arestas contidas no menor ciclo homologicamente não-trivial. Os operadores também são definidos de modo semelhante aos operadores de Kitaev. Ilustraremos a construção de Freedman e Meyer com o código $[[9,1,3]]$ equivalente ao código de Shor.

A Figura 4.8 mostra uma celulação de $\mathbb{R}P^2$ com nove arestas, definindo um código que codifica um qubit em nove. Nesse diagrama, pontos antípodas no círculo são identificados. Note que, o comprimento de ambos os ciclos mínimo fundamental e mínimo fundamental dual é 3, portanto $d = 3$. Verifica-se que esse código é equivalente ao código de Shor comparando seus operadores estabilizadores.

4.3.2 Códigos tóricos $[[d^2+1,2,d]]$

Em [13], Bombin e Martin-Delgado consideram o código de Kitaev $l \times l$ como a *região fundamental* de um reticulado do toro, que chamaremos de sub-reticulado para não confundir. Translações dessa

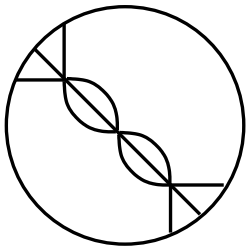

Figura 4.8: Código $[[9,1,3]]$ equivalente ao código de Shor.

região fundamental resultam no reticulado quadrado do toro $\mathbb{Z}\times\mathbb{Z}$, veja Figura 4.9. Os parâmetros e propriedades do código tórico permanecem os mesmos. Além disso, podemos interpretar a distância mínima do código como sendo o menor número de arestas do reticulado dual entre duas regiões fundamentais distintas. Na Figura 4.9 essas regiões são demarcadas pelas retas em negrito e têm a marcação X como um representante.

Para definir seus códigos, Bombin e Martin-Delgado utilizam outro sub-reticulado regular para tesselar o toro $\mathbb{Z}\times\mathbb{Z}$, veja Figura 4.9. Esse novo sub-reticulado tem esferas de Lee de raio r como região fundamental. Como foi mencionando no exemplo 2.3, l esferas de Lee de raio t, em duas dimensões, podem ser usadas para tesselar o toro $l\times l$, onde $l=2t^2+2t+1$ e $t=1,2,\ldots$, [36]. Logo essa tesselação pode ser estendida para o reticulado $\mathbb{Z}\times\mathbb{Z}$. Este sistema de reticulados usado em [13] fornece códigos com parâmetros $[[d^2+1,2,d]]$ que demandam um pouco mais da metade do número de qubits e mantém as mesmas propriedades do código original de Kitaev, como por exemplo, os operadores vértice e face agindo em quatro qubits.

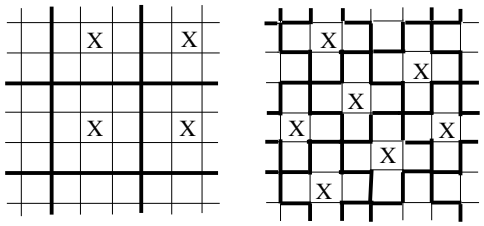

Figura 4.9: Reticulados do código de Kitaev e do código de Bombin e Martin-Delgado com $d=3$.

Capítulo 5

Novos Códigos Quânticos Tóricos

No capítulo 3, foi mostrado que uma nova interpretação do código de Kitaev, proposta por Bombin e Martin-Delgado, proporciona uma melhora significativa quanto ao comprimento do código, resultando em uma melhor taxa de codificação. Esta abordagem baseia-se em uma nova região fundamental do reticulado regular, e mantém as mesmas propriedades dos códigos de Kitaev.

A partir disso, vimos que é possível gerar vários outros códigos quânticos tóricos de acordo com a possibilidade de cobrir o reticulado quadrado do toro, por determinados formatos ou regiões fundamentais. Esses formatos são conhecidos como *poliminós* [1], [37], união de uma certa quantidade de quadrados unitários. Classicamente, os poliminós já foram usados para determinar códigos *close-packed*, [36], que são códigos definidos por tesselações de um reticulado através de translações de um determinado poliminó. Lembramos que uma tesselação é uma cobertura do plano completo por polígonos (neste caso, por poliminós) iguais sem superposições, encontrando-se somente ao longo de arestas completas ou em vértices (veja Seção 6.2).

Nossa proposta utiliza a estrutura algébrica de grupos e também a estrutura de ideais de anéis de inteiros Gaussianos para gerar um método de obtenção de tais tesselações. Também mostramos uma maneira ainda mais geral de obter essas tesselações através de uma abordagem combinatorial. Dentre esses códigos é possível identificar diversas classes de códigos tóricos, inclusive reproduzir os códigos de Kitaev e Bombin e Martin-Delgado. Com respeito ao comprimento do código e taxa de codificação, obtivemos uma classe de códigos $[[d^2, 2, d]]$ melhor que os anteriores.

Na Seção 5.1 apresentamos a relação entre formas quadráticas e reticulados, e definimos poliminós. A Seção 5.2 é dedicada ao problema de determinar essas novas tesselações por poliminós de um ponto de vista algébrico, além disso reproduzimos as classes de códigos tóricos conhecidas e apre-

[1] Em inglês o termo usado é poliomino que é uma generalização de domino e foi inventado por Solomon W. Golomb em 1953. Em português o termo é uma generalização de dominó, portanto dizemos poliminó.

sentamos novas classes. Na Seção 5.3 abordamos o mesmo problema através de um ponto de vista combinatorial, por meio de determinante de matrizes quadradas 2×2.

5.1 Formas Quadráticas, Reticulados e Poliminós

Antes de propor a construção de códigos quânticos tóricos, se faz necessário uma breve revisão de conceitos matemáticos como formas quadráticas, reticulados e poliminós. Para maiores informações, sugerimos as referências [20, 37, 75].

5.1.1 Formas Quadráticas e Reticulados

Uma forma quadrática Q em n variáveis, é um polinômio homogêneo de grau dois

$$Q = a_{11}x_1^2 + a_{12}x_1x_2 + \ldots + a_{n,n-1}x_nx_{n-1} + a_{nn}x_n^2 = \sum_{1 \leq i,j \leq n} a_{ij}x_ix_j,$$

onde $a_{ij} \in \mathbb{R}$. Fazendo $X = (x_1, \ldots, x_n)^T$ e $A = \{a_{ij}\}$ uma matriz $n \times n$, podemos escrever

$$Q = X^T AX.$$

O estudo das formas quadráticas é muito antigo, desde os gregos, passando por Fermat e Lagrange, entre outros. Particularmente, estamos interessados na forma quadrática $x^2 + y^2$, onde x e y são números inteiros. O problema de um inteiro poder ser expresso como uma soma de quadrados de inteiros do tipo $x^2 + y^2$ foi tratada originalmente no Teorema de Pitágoras. Por volta de 1621, Fermat conjecturou e comprovou que um número primo p pode ser escrito como a soma de dois quadrados inteiros se, e somente se, $p = 2$ ou p é do tipo $4\kappa + 1$. Euler demonstrou definitivamente esse resultado por volta de 1754. A teoria geral de todas as formas quadráticas $ax^2 + bxy + by^2$ deve-se a Lagrange que deu início a classificação de formas quadráticas relacionando-as a geometria de certos pontos regularmente espaçados no plano, os *reticulados*, [75].

Os reticulados têm sido bastante utilizados na teoria das comunicações. Sua principal aplicação está relacionada ao problema de codificação de canal, que é equivalente ao problema de empacotamento de esfera. Em geral, reticulados podem ser usados para a construção de códigos em n dimensões para o problema de codificação de canal ou para quantização de vetores n-dimensionais.

Como foi mencionado no capítulo 4, um reticulado Λ é um subconjunto discreto infinito de $\mathbb{R}^n$ que forma um grupo aditivo sob adição usual de vetores.

Se Λ é um reticulado em um espaço n-dimensional, então existem vetores linearmente independentes $\nu_1, \nu_2, \ldots, \nu_n$ tais que Λ consiste de todos os pontos da forma $\xi = \sum_{i=1}^{n} x_i\nu_i$, onde $x_i \in \mathbb{Z}$. Tal conjunto de vetores $\beta = \{\nu_1, \nu_2, \ldots, \nu_n\}$ é chamado uma *base* de Λ, [75].

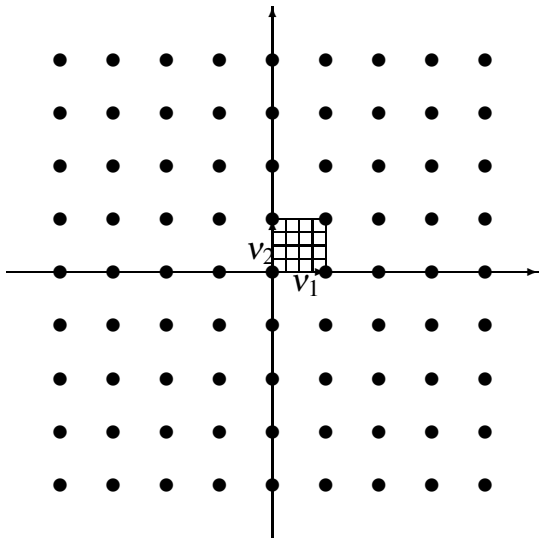

Figura 5.1: Reticulado $\mathbb{Z}^2$ gerado por v_1 e v_2.

Uma *região fundamental* para um reticulado Λ é um bloco de construção que quando transladado muitas vezes pelos elementos de Λ preenche o espaço completo com apenas um ponto do reticulado em cada cópia. Existem diferentes formas de escolher uma base e uma região fundamental para um reticulado Λ, mas o volume da região fundamental é unicamente determinado por Λ, [20]. O volume da região fundamental é $|det(B)|$, onde B é a matriz quadrada formada pelos vetores da base β de um reticulado.

Por exemplo, o reticulado $\Lambda = \mathbb{Z}^2$ é gerado pelos vetores $v_1 = (1,0)$ e $v_2 = (0,1)$ com região fundamental descrita na Figura 5.1, e $B = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Então, $det(B) = 1$. Ou seja, uma região fundamental do reticulado $\mathbb{Z}^2$ é um quadrado com área 1.

Formas quadráticas fornecem uma linguagem alternativa para estudos de reticulados, especialmente conveniente para investigar propriedades aritméticas, [20].

Em termos gerais, seja Λ um reticulado no espaço n-dimensional $\mathbb{R}^n$, com vetores base $v_1, \ldots, v_n$, formando as linhas de uma matriz geradora B. Um vetor reticulado qualquer $\xi = (\xi_1, \ldots, \xi_n) \in \Lambda$ pode ser escrito como $\xi = x_1 v_1 + \ldots + x_n v_n = xB$, onde x_i são inteiros e $x = (x_1, \ldots, x_n)$. A norma desse vetor é $N(\xi) = N(x_1 v_1 + \ldots + x_n v_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j v_i \cdot v_j = xBB^T x^T = xAx^T = f(x)$, onde a norma é definida como $N(\xi) = \xi \xi^T$ e $A = BB^T$ é chamada uma matriz *Gram* para Λ. Visto como uma função das n variáveis $\xi_1, \ldots, \xi_n$, $f(x)$ é uma forma quadrática associada ao reticulado.

Por exemplo, dada $B = \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$, a matriz *Gram* é $A = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}$. Assim uma forma quadrática associada ao reticulado hexagonal é $x_1^2 + x_1x_2 + x_2^2$. Já o reticulado cúbico n-dimensional $\mathbb{Z}^n$ tem como matriz geradora a matriz identidade de ordem n, I_n, e a forma quadrática correspondente é $x_1^2 + x_2^2 + \ldots + x_n^2$, [20].

Em particular, o reticulado quadrado bidimensional $\mathbb{Z}^2$ tem matriz geradora $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, e a forma quadrática correspondente é $x_1^2 + x_2^2$.

5.1.2 Poliminós

A expressão *poliminó* foi inventada em 1953 por Solomon W. Golomb. O termo poliminó é uma generalização de "dominó" o formato que inclui dois quadrados com tamanhos iguais e um lado em comum. Um dominó tem somente o formato de um retângulo. Um trominó é um poliminó formado por três quadrados e existem dois formatos de trominós, assim como existem quatro formatos de tetrominós, doze pentominós e trinta e cinco hexominós distintos, e assim por diante, [37].

Padrões poliminós são exemplos de geometria combinatorial, ramo da matemática relacionada com as maneiras na qual formatos geométricos podem ser combinados. A princípio poliminós tinham um caráter mais próximo a matemática recreativa, porém já foram usados em codificação clássica para obtenção de códigos *close-packed*. Um código *close-packed* corresponde a qualquer tesselação de um toro $m \times m$ por translações de um dado formato poliminó, [36].

Um modelo especial de poliminó é a esfera de Lee. Um reticulado quadrado do toro $m \times m$ pode ser tesselado por m esferas de Lee de raio $t = 1, 2, \ldots$, desde que $m = 2t^2 + 2t + 1$, [36]. Esse tipo de tesselação foi usada para gerar códigos clássicos perfeitos, como vimos no exemplo 2.3, cujo padrão de correção de erros é simétrico, [36]. Por outro lado, a mesma tesselação também foi usada para determinar códigos quânticos $[[d^2 + 1, 2, d]]$ em [13].

5.2 Conjunto dos Representantes dos Poliminós - Uma Abordagem Algébrica

Algebricamente, podemos caracterizar o código de Kitaev como o conjunto de classes laterais do grupo quociente $\mathbb{Z}^2/m\mathbb{Z}^2 \cong \mathbb{Z}_m \times \mathbb{Z}_m$. As identificações dos lados opostos da região delimitada por $\mathbb{Z}_m \times \mathbb{Z}_m$ resulta na identificação com o toro plano. A área associada ao reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$ é m^2, e como cada aresta pertence simultaneamente a duas faces quadradas do reticulado, temos $2m^2$ arestas, ou seja, constata-se que $n = 2m^2$ qubits. Além disso, os qubits a serem codificados estão relacionados

aos ciclos fundamentais da superfície, e portanto $k = 2$, e a distância mínima do código por ser definida como o número de arestas no menor ciclo homologicamente não-trivial, donde $d = m$.

Agora, observando a Figura 4.9 sob o ponto de vista de Bombin e Martin-Delgado, o código passa a ser definido na região fundamental que transladada cobre todo o reticulado. Assim, temos que o comprimento do código passa a ser o número de arestas da região fundamental, levando em consideração que não se deve contar duas vezes uma mesma aresta; a dimensão do código é $k = 2$, pois depende da topologia da superfície; e a distância do código, se observada na região fundamental, equivale a distância entre duas regiões vizinhas. Então, se considerarmos qualquer tesselação do toro dada por translações de uma região fundamental, ou melhor, de um poliminó, podemos definir um código quântico associado a essa região similarmente ao que foi feito em [13].

A princípio, qualquer tesselação pode ser considerada para a construção de tais códigos, desde que a área do poliminó divida a área do reticulado quadrado $\mathbb{Z}_m \times \mathbb{Z}_m$. Ou seja, a área do poliminó deve ser igual a um divisor de m^2. Observe que, para m igual a um número primo, os únicos divisores são 1 (caso trivial) e m, além do próprio número. Por estarmos interessados em uma construção mais geral possível, iremos então considerar apenas os casos onde o poliminó tem área igual a m. Por exemplo, para $m = 5$ a Figura 5.2 mostra dois modelos de poliminós que tesselam o reticulado $\mathbb{Z}_5 \times \mathbb{Z}_5$. Encontrar esses formatos é um problema combinatorial. A importância do formato dos poliminós está relacionada aos padrões de correção de erros do código, [36].

Podemos tornar o problema de encontrar os poliminós da tesselação mais sistemático se determinarmos o conjunto de representantes desses poliminós, denotados nas figuras pela marca X. Esses pontos são dados pelas coordenadas $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_m$ e nos indica onde deve haver um poliminó, o que facilita a construção da tesselação. Por exemplo, na Figura 5.2 os representantes são dados pelas coordenadas $(0,0), (2,1), (4,2), (1,3)$ e $(3,4)$. Para resolver esse problema, propomos uma abordagem algébrica via teoria de grupos.

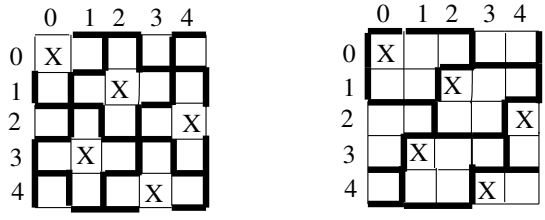

Figura 5.2: Duas representações de regiões com área 5.

Esse conjunto de representantes corresponde a um código reticulado clássico que é um subconjunto de pontos de um reticulado Λ. Ou seja, é um subespaço vetorial de $\mathbb{Z}_m \times \mathbb{Z}_m$ ou mais precisamente um

$\mathbb{Z}_m$-módulo, que denotaremos por $\mathscr{A}$. Obviamente, para que a área do poliminó seja m, a cardinalidade de $\mathscr{A}$ deve ser m.

Sabemos que a forma quadrática associada ao reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$ é dada por x^2+y^2. Baseados nisso, usaremos a igualdade $x^2+y^2=m$ para encontrar os vetores reticulados $(x,y) \in \mathscr{A}$ com $x,y \in \mathbb{Z}$. Isso implica que a área do poliminó é de fato m. Através da soma usual de vetores, é possível achar todos os elementos de $\mathscr{A}$, mas observe que a operação deve ser realizada módulo m, para que os pontos estejam dentro do reticulado $\mathbb{Z}_m \times \mathbb{Z}_m$. Essa operação corresponde ao deslocamento de x unidades horizontalmente e y unidades verticalmente nas células do reticulado. Se x ou y for negativo, o sinal negativo indica o deslocamento no sentido oposto.

Note que, o conjunto dos representantes dos poliminós pode ser visto também como um subgrupo do grupo aditivo $(\mathbb{Z}_m \times \mathbb{Z}_m, +)$, e com isso podemos trabalhar com a estrutura de grupo. Nas proposições 1 e 2 veremos que, se x e y são relativamente primos tais que $m=x^2+y^2$, então $\mathscr{A}=\langle (x,y) \rangle$, do contrário, $\mathscr{A}=\langle (x,y),(-y,x) \rangle$.

Proposição 1 *Se x e y são inteiros primos entre si, então a ordem do grupo gerado pelo elemento (x,y) é m, ou seja, $o(\langle (x,y) \rangle)=m$.*

Demonstração: Obviamente, temos que $mx=my=0$, e portanto $m(x,y)=(0,0)$. Agora, suponha que existe $\tau \in \mathbb{N}$, com $0<\tau<m$, tal que $\tau(x,y)=(0,0)$. Então $\tau x=\tau y=0$. Como x e y são relativamente primos, então existem inteiros α e β tais que $x\alpha+y\beta=1$. Segue que $\tau=\tau x\alpha+\tau y\beta=0$, o que contradiz a hipótese $0<\tau<m$. Logo, $m=o(\langle (x,y) \rangle)$. ∎

O resultado vale para todo par (x,y) tal que $mdc(x,y)=1$. Em particular, vale quando $mdc(x,y)=1$ e $m=x^2+y^2$. Obviamente, se $x \neq 0$ e $y=0$ então $o(\langle (x,y) \rangle)=o(x)=x$, ou se $x=0$ e $y \neq 0$ então $o(\langle (x,y) \rangle)=o(y)=y$.

Os seguintes fatos são facilmente demonstrados:

1. Se $mdc(x,y)=\delta \neq 0$ então $mdc(\frac{x}{\delta},\frac{y}{\delta})=1$.

2. Se $m=x^2+y^2$ e $mdc(x,y)=\delta \neq 0$, com $x \neq 0$ e $y \neq 0$, então δ divide m, uma vez que $\delta \mid x$ e $\delta \mid y$, e assim $\delta \mid x^2$ e $\delta \mid y^2$. Logo, $\delta \mid (x^2+y^2)=m$. Portanto, o quociente m/δ faz sentido.

Proposição 2 *Se x e y não são relativamente primos, então $o(\langle (x,y) \rangle)=\frac{m}{\delta}$, onde $\delta=mdc\{x,y\}$.*

Demonstração: Como $mdc\{x,y\}=\delta$, segue que $x=x_0\delta$ e $y=y_0\delta$, para algum $x_0,y_0 \in \mathbb{Z}$. Logo,

$$\frac{m}{\delta}(x,y)=(\frac{m}{\delta}x_0\delta,\frac{m}{\delta}y_0\delta)=(mx_0,my_0)=(0,0).$$

Agora, suponha por absurdo que exista $0 < \tau < \frac{m}{\delta}$ tal que $\tau(x,y) = (0,0)$. Assim, $\tau x = \tau y = 0$, e $0 < \tau\delta < m$. Por outro lado, como $mdc\{x,y\} = \delta$, então existem $\alpha, \beta \in \mathbb{Z}$ tais que $x\alpha + y\beta = \delta$. Logo, $\tau x\alpha + \tau y\beta = \tau\delta$, daí $\tau\delta = 0$ contradizendo a hipótese $0 < \tau\delta < m$. Conclui-se que $o(\langle(x,y)\rangle) = \frac{m}{\delta}$. ∎

Observe que o resultado vale quando $mdc(x,y) \neq 0$ divide m. Em particular, vale quando $m = x^2 + y^2$.

Como desejamos que $|\mathscr{A}| = m$, então nos casos em que x e y são relativamente primos, onde $m = x^2 + y^2$, consideramos o grupo $\mathscr{A}$ igual ao grupo cíclico $\langle(x,y)\rangle$. Nos casos onde x e y não são relativamente primos, ou seja $mdc(x,y) = \delta \neq 0, 1$, então iremos considerar o grupo $\mathscr{A}$ igual ao grupo gerado por dois elementos $\langle(x,y),(-y,x)\rangle$ cuja cardinalidade é m.

Enfatizamos que nos casos onde $m = x^2 + y^2$ com $mdc(x,y) = 1$, temos que o conjunto dos representantes dos poliminós, $\mathscr{A}$, é um código perfeito no sentido de ter apenas um representante X em cada linha ou coluna, [21].

Conhecido o subespaço formado pelos representantes, é possível escolher os poliminós que podem tesselar o reticulado e definir o código quântico associado. O comprimento do código proposto é dado pelo número de arestas do poliminó. Como o poliminó tem área m, e cada aresta pertence simultaneamente a duas faces quadradas do reticulado original do toro, temos que a quantidade efetiva de arestas é $n = 2m$. A dimensão do código é $k = 2$ devido a este código ser construído no toro. E a distância mínima do código é dada pela menor distância entre dois representantes de poliminós distintos, ou seja, é o número mínimo de arestas no reticulado dual entre dois representantes dos poliminós. Segue que essa distância é dada por $d_M = |x| + |y|$, e é conhecida como *distância de Mannhein*. Portanto, os parâmetros dos códigos quânticos gerados por essas tesselações são $[[2m, 2, d_M]]$.

Enfatizamos que para cada tesselação de um reticulado $\mathbb{Z}_m^2$, o poliminó pode ter formatos diferentes, porém os parâmetros n, k e d não se alteram, ou seja, o código quântico gerado é o mesmo. Entretanto, o formato do poliminó influencia no padrão de correção de erros. De uma maneira geral, podemos considerá-lo como a junção de dois quadrados: $x \times x$ com $y \times y$. No entanto, pode-se encontrar outros poliminós que tesselam o mesmo reticulado, esse é um problema de geometria combinatorial. Decidir qual o melhor formato para o poliminó depende do tipo de grafo associado ao canal discreto sem memória, por exemplo, se o canal for simétrico então é melhor usar poliminós simétricos em relação à marca X (nem sempre isso será possível), porém se o canal não for simétrico, então é melhor escolher um poliminó mais adequado.

Com essa construção é possível reproduzir códigos tóricos já existentes, assim como gerar classes novas.

5.2.1 Reprodução dos códigos de Bombin e Martin-Delgado

Quando $m = 2t^2 + 2t + 1$, para $t = 1, 2, 3, \ldots$, reproduzimos os códigos de Bombin e Martin-Delgado. Com efeito, se $m = 2t^2 + 2t + 1$, então podemos escrevê-lo como soma de quadrados da seguinte forma $m = (t+1)^2 + t^2$. Ou seja, $x = t + 1$ e $y = t$. Assim, x e y são primos entre si, portanto $\mathscr{A} = \langle (x, y) \rangle$. Segue que $d = |t+1| + |t| = 2t + 1$, e $n = 2m = 2(2t^2 + 2t + 1) = 4t^2 + 2d = 4\frac{(d-1)^2}{4} + 2d = (d-1)^2 + 2d = d^2 + 1$. Portanto $[[d^2 + 1, 2, d]]$. O formato do poliminó pode ser a junção de quadrados como visto anteriormente ou pode ser também a esfera de Lee de raio t utilizada em [13].

Exemplo 5.1 *Se $m = 5$, então as únicas soluções para $x^2 + y^2 = 5$ são $x = \pm 2$ e $y = \pm 1$ ou vice-versa. Sem perda de generalidade, digamos que $\mathscr{A} = \langle (2,1) \rangle$, ou seja, $\mathscr{A} = \{(0,0), (2,1), (4,2), (1,3)$ e $(3,4)\}$. Note que as operações são feitas módulo 5. Esses elementos representam os poliminós, que neste caso, podem ser as esferas de Lee de raio $t = 1$ ou também podem ser quadrados 2×2 junto com quadrados 1×1, veja Figura 5.2. Como $d = |2| + |1| = 3$, obtemos um código $[[10, 2, 3]]$.*

5.2.2 Reprodução dos códigos de Kitaev

Quando m é um quadrado perfeito, as únicas soluções para $m = x^2 + y^2$ são $x = \pm\sqrt{m}, y = 0$ ou vice-versa. Sem perda de generalidade, consideramos $\mathscr{A} = \langle (\sqrt{m}, 0), (0, \sqrt{m}) \rangle$. Marcando os representantes no reticulado obtemos poliminós quadrados $\sqrt{m} \times \sqrt{m}$. Temos que os parâmetros dos códigos são $n = 2m$, $k = 2$ e $d = |\sqrt{m}|$, logo $n = 2d^2$. Portanto reproduzimos os parâmetros dos códigos tóricos de Kitaev $[[2d^2, 2, d]]$.

Exemplo 5.2 *Para $m = 4$, temos que as únicas soluções para $4 = x^2 + y^2$ são $x = \pm 2$ e $y = 0$ ou vice-versa. Sem perda de generalidade, considere $x = 2$ e $y = 0$. O vetor $(2,0)$ nos proporciona duas marcas X no reticulado, $(2,0), (0,0)$, enquanto o vetor $(0,2)$ produz as marcas em $(0,2), (0,0)$. Como $\mathscr{A}$ deve ser um subgrupo, então a soma dos seus elementos também pertence a $\mathscr{A}$, ou seja, $\mathscr{A} = \{(0,0), (2,0), (0,2), (2,2)\}$. Os poliminós são definidos como quadrados 2×2, veja Figura 5.3. Contando o número de arestas do poliminó temos que $n = 8$. Além disso, pode-se verificar que a distância é $d = |2| + |0| = 2$. Logo, temos um código $[[8, 2, 2]]$.*

5.2.3 Nova classe de códigos tóricos $[[d^2, 2, d]]$

Considere agora os valores de m que são o dobro de um quadrado perfeito, ou seja, $m = x^2 + x^2$. Neste caso, o conjunto dos representantes dos poliminós é gerado por dois elementos (x, x) e $(-x, x)$.

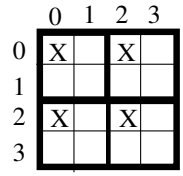

Figura 5.3: Código de Kitaev $[[8,2,2]]$.

Temos que $d = 2x$ e $n = 2m = 2(2x^2) = 4x^2 = d^2$. Logo obtemos um código tórico com parâmetros $[[d^2,2,d]]$. Em termos de taxa de codificação este código é melhor que os anteriores, $k/n = 1/d$. Um dos possíveis poliminós neste caso é um retângulo $2x \times x$. Esses poliminós não são simétricos quanto ao representante X, por isso esse tipo de código pode ser útil em um canal não simétrico.

Exemplo 5.3 *Seja* $m = 8$. *Temos que as únicas soluções para* $8 = x^2 + y^2$ *são* $x, y = \pm 2$. *Sem perda de generalidade, considere* $x = y = 2$. *Assim,* $\mathscr{A} = \langle (2,2),(-2,2)\rangle = \{(0,0),(2,2),\ (4,4),\ (6,6),(6,2),(2,6),(0,4),(4,0)\}$. *Os poliminós podem ser quadrados* 2×2 *juntos a quadrados* 2×2*, ou seja, um retângulo* 4×2. *Obtemos um código* $[[16,2,4]]$. *Na Figura 5.4 mostramos dois modelos de tesselações para esse exemplo.*

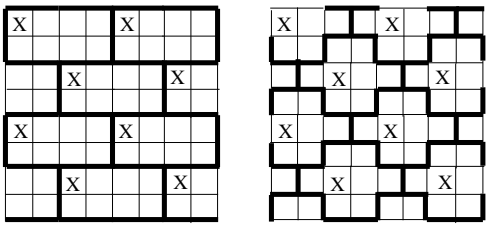

Figura 5.4: Duas representações do código $[[16,2,4]]$.

5.2.4 Outras classes de códigos tóricos

Podemos obter várias classes novas de códigos tóricos impondo condições a x e y ou m. Por exemplo, se considerarmos os valores de m tais que $m = x^2 + y^2$, onde $y = x - 2$. Temos que $d = d_M = 2x - 2$ e $n = 2m = 2(x^2 + (x-2)^2) = 2(2x^2 - 4x + 4) = 4(x^2 - 2x + 2)$. Substituindo o valor de $x = \frac{d+2}{2}$, seque que

$$\begin{aligned} n &= 4[\frac{(d+2)^2}{4} - 2\frac{d+2}{2} + 2] \\ n &= 4[\frac{d^2+4d+4}{4} - d] \\ n &= 4[\frac{d^2+4d+4-4d}{4}] \\ n &= d^2 + 4. \end{aligned}$$

Assim, obtemos a classe de códigos $[[d^2+4,2,d]]$. Mais geralmente, se considerarmos $y = x - \varsigma$, temos a classe de códigos $[[d^2+\varsigma^2,2,d]]$.

Pode-se encontrar outras classes de códigos tóricos se assumirmos que um dos valores x ou y seja igual a 1. Digamos $y = 1$. Assim, $d = d_M = x+1$ e $n = 2m = 2(x^2+1) = 2[(d-1)^2+1] = 2(d-1)^2+2$. Resulta na classe de códigos $[[2(d-1)^2+2,2,d]]$. Em geral, se $y = \varsigma$, então obtemos a classe de códigos $[[2(d-\varsigma)^2+2\varsigma^2,2,d]]$.

Se x for um múltiplo de y, por exemplo, $x = 2y$, temos que $d = d_M = 3y$ e $n = 2m = 2(5y^2) = 10y^2 = 10\frac{d^2}{9}$. No caso geral, onde $x = \varsigma y$, temos a classe de códigos $[[2(\varsigma^2+1)\frac{d^2}{(\varsigma+1)^2},2,d]]$.

Assim como essas classes, podemos encontrar muitas outras de acordo com as condições sobre x, y e m.

5.2.5 Anel de inteiros Gaussianos

Outra maneira de obter sistematicamente o conjunto de representantes de poliminós é utilizando a estrutura algébrica de anel. Entretanto, como essa estrutura é mais restritiva do que a de grupo, obtemos menos códigos.

Considere a aplicação

$$\eta : \mathbb{Z}_m^2 \to \mathbb{Z}_m[i],$$

dada por $(x,y) \mapsto x+y\cdot i$, onde $\mathbb{Z}[i] = \{x+y\cdot i; x,y \in \mathbb{Z}\}$ é o anel de inteiros de Gauss. Considerando o grupo aditivo $(\mathbb{Z}[i],+)$ e a operação de soma realizada módulo m, temos que η é um isomorfismo.

O anel $\mathbb{Z}[i]$ não foi escolhido de modo aleatório. A partir de um método gerado por Minkowski pode-se obter reticulados no $\mathbb{R}^n$ através de um homomorfismo, conhecido como homomorfismo canônico, de um corpo de números $\mathbb{K}$ do $\mathbb{R}^n$, de modo que a imagem de um ideal não-nulo do anel de inteiros $I_{\mathbb{K}}(\mathbb{Z})$ por este homomorfismo seja um reticulado de posto n no $\mathbb{R}^n$. Os reticulados obtidos dessa maneira dependem diretamente do anel de inteiros de um corpo de números. Os principais parâmetros desse reticulado podem ser obtidos via teoria algébrica dos números, através de propriedades de $\mathbb{K}$, [65].

Considere o caso particular quando $\mathbb{K} = \mathbb{Q}[i]$ é a extensão quadrática de $\mathbb{Q}$ associada ao inteiro livre de quadrados -1. Seu grupo de Galois $\mathscr{G}$ é formado por dois elementos σ_1 e σ_2, onde $\sigma_1(x+y\cdot i) = x+y\cdot i$ e $\sigma_1(x+y\cdot i) = x-y\cdot i$, para todo $x,y \in \mathbb{Q}$. O anel de inteiros $\mathbb{Z}[i]$ de $\mathbb{Q}[i]$ é conhecido como anel de inteiros de Gauss, e tem norma $N(x+y\cdot i) = x^2+y^2$, que é a forma quadrática associada ao reticulado quadrado. O reticulado obtido a partir de $\mathbb{Z}[i]$ é o reticulado quadrado $\mathbb{Z}^2$. Observe que $(\mathbb{Z}[i],+,\cdot,N)$ é um domínio Euclidiano, e portanto todo ideal de $\mathbb{Z}[i]$ é principal. Além disso, se um

ideal de $\mathbb{Z}[i]$ for um ideal primo, então será um ideal maximal, [76].

Classicamente, subconjuntos finitos $\mathscr{A}_p[i] \subset \mathbb{Z}[i]$ com p elementos, onde $p \equiv 1(mod 4)$, foram usados como alfabetos de códigos, [57]. Esses subconjuntos $\mathscr{A}_p[i]$ correspondem aos quocientes $\mathbb{Z}[i]/\mathscr{I}$, onde $\mathscr{I}$ é um ideal primo de $\mathbb{Z}[i]$, e podem ser vistos como um corpo isomorfo a $\mathbb{F}_p$, o corpo de Galois de ordem p.

Se $\mathscr{A} = \langle (x,y) \rangle$ com $mdc(x,y) = 1$, então a imagem de $\mathscr{A}$ pelo isomorfismo η é um ideal $\mathscr{I}$ de $\mathbb{Z}[i]$, com m elementos. De fato, $\mathscr{A} = \langle (x,y) \rangle$ implica que $\mathscr{I} = \langle z \rangle$, onde $z = x + y \cdot i$. Ou seja, $\mathscr{I}$ é um ideal principal de ordem m. Se $m = p$ é um primo ímpar tal que $p \equiv 1(mod 4)$, temos que $\mathscr{I}$ é um ideal primo e, portanto, é maximal, ou seja, $\mathscr{I}$ é o maior ideal em $\mathbb{Z}[i]$ que contém o conjunto de representantes dos poliminós. Além disso, o quociente $\mathbb{Z}[i]/\mathscr{I}$ é um corpo, estrutura algébrica bastante utilizada para definir códigos clássicos.

Em $\mathbb{Z}_m^2$, para encontrarmos os valores de x e y fazemos a forma quadrática $x^2 + y^2$ ser igual a m. Analogamente, em $\mathbb{Z}[i]$, fazemos a norma $N(z) = x^2 + y^2$ ser igual a m e encontramos os valores de x e y. Os representantes no reticulado correspondem às coordenadas quando partimos da célula $(0,0)$ e deslocamos x unidades horizontalmente e y unidades verticalmente nas células do reticulado. Se algum valor de x e y for negativo, então o deslocamento é feito no sentido oposto. Note que, as operações em $\mathbb{Z}[i]$ são realizadas módulo m para restringirmos o reticulado a $\mathbb{Z}_m \times \mathbb{Z}_m$.

5.3 Conjunto dos Representantes dos Poliminós - Uma Abordagem Combinatorial

Dado um reticulado $m \times m$, do ponto de vista combinatorial, o problema de determinar o vetor reticulado $(x,y) \in \mathbb{Z}_m \times \mathbb{Z}_m$ que representa um poliminó pode ser resolvido através de uma matriz quadrada $\mathrm{A} = \begin{bmatrix} \mathrm{a} & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{bmatrix}$ cujo determinante é m.

As linhas da matriz A definem o deslocamento nas células do reticulado para determinar os representantes dos poliminós da seguinte maneira: a unidades para a direita e b unidades para baixo; e c unidades para a direita e d unidades para baixo. Se algum desses valores for negativo, o deslocamento é feito no sentido oposto. Essa operação também pode ser vista como soma usual de vetores módulo m, onde consideramos o conjunto de vetores gerado por (a,b) e por (c,d).

Assim, obtemos um conjunto de m vetores reticulados que correspondem aos representantes dos poliminós, $\mathscr{A}$. Se mudarmos os valores de a, b, c e d de forma que $det(\mathrm{A}) = m$, o conjunto de representantes dos poliminós permanece com m elementos, porém podem estar em posições diferentes no reticulado. Logo, cada conjunto de posições nos fornece uma tesselação por poliminós que podem

ser diferentes. Apesar do formato do poliminó não influenciar nos parâmetros do código quântico, a posição dos representantes influencia no próprio formato do poliminó e na distância do código. Além disso, a distância agora deve ser observada no reticulado. Em alguns casos será dada por $d = min\{|a|+|b|,|c|+|d|\}$, porém existem casos onde a distância efetiva é menor que este mínimo.

Exemplo 5.4 *Para $m = 3$, temos que $A = \begin{bmatrix} 3 & 3 \\ 1 & 2 \end{bmatrix}$ tem determinante 3. Note que $d = min\{|3|+|3|,|1|+|2|\} = 3$, porém na Figura 5.5 pode-se verificar que $d = 2$. Neste caso, temos um código $[[6,2,2]]$. Obtemos o mesmo conjunto de representantes, portanto o mesmo código $[[6,2,2]]$, se tomarmos a matriz $A = \begin{bmatrix} 1 & -1 \\ 2 & 1 \end{bmatrix}$, cujo determinante é 3. Neste caso, $d = min\{|1|+|-1|,|2|+|1|\} = 2$.*

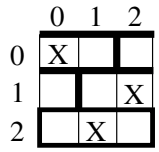

Figura 5.5: Código $[[6,2,2]]$.

Existem alguns casos que recaem nos mesmos valores obtidos através da abordagem algébrica, a saber quando a,b,c e d são as soluções $(\pm x,\pm y)$ ou $(\pm y,\pm x)$ de $x^2+y^2=m$, assim A $= \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$. Neste caso, a distância mínima do código é a distância de Mannheim. Podemos reproduzir da mesma forma os códigos de Kitaev, Bombin e Martin-Delgado, a classe $[[d^2,2,d]]$ e as demais classes da subseção 5.2.4.

Exemplo 5.5 *Para reproduzir o Exemplo 5.1 podemos considerar a matriz $A = \begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}$. Então, $det(A) = 5$ e os vetores reticulados que representam os poliminós são $(0,0),(2,1)$, $(4,2),(1,3)$ e $(3,4)$.*

Exemplo 5.6 *Para reproduzir o Exemplo 5.2 podemos considerar a matriz $A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$. Assim, $det(A) = 4$ e os vetores reticulados são $(0,0),(2,0),(0,2)$ e $(2,2)$.*

Exemplo 5.7 *O Exemplo 5.3 pode ser obtido da matriz $A = \begin{bmatrix} 2 & 2 \\ -2 & 2 \end{bmatrix}$. Logo, $det(A) = 8$ e os vetores reticulados que representam os poliminós são $(0,0)$, $(2,2)$, $(4,4)$, $(6,6)$, $(6,2)$, $(2,6)$, $(0,4)$, $(4,0)$.*

Se considerarmos a e b da matriz A como sendo respectivamente os valores x e y obtidos através do método algébrico, com $mdc(x,y) = 1$, a partir da relação $xd - yc = m$ podemos determinar todos os possíveis valores para c e d. Todas essas soluções, exceto as triviais, onde c ou d assumem os valores cônguros a 0 $(mod\ m)$, nos dão o mesmo conjunto de representantes, isto é, $\langle(x,y)\rangle = \langle(c,d)\rangle$.

Exemplo 5.8 *Para $m=5$, vimos no Exemplo 5.1 que uma solução para (x,y) é $(2,1)$. Então considere $(a,b)=(2,1)$. Assim, $2d-c=5$, e algumas possíveis soluções para (c,d) são $(-3,1),(-1,2),(1,3)$ ou $(3,4)$. A matriz $A=\begin{bmatrix} 2 & 1 \\ w & z \end{bmatrix}$ com esses valores de c e d tem determinante 5. O conjunto de vetores reticulados gerados por $(-3,1),(-1,2),(1,3)$ ou $(3,4)$ é igual ao conjunto de vetores reticulados gerados por $(2,1)$, lembrando que as somas são feitas módulo 5. Portanto, obtemos o código $[[10,2,3]]$ do Exemplo 5.1.*

Através do método combinatorial é possível cobrir casos que não são possíveis de ser reproduzidos algebricamente. Por exemplo, para $m=p$ um primo ímpar tal que $p=4\kappa+3$. Esses valores não podem ser escritos como soma de quadrados, na verdade obedecem a outras formas quadráticas, ou melhor, pertencem a outros anéis de inteiros e por isso têm uma norma diferente da soma de quadrados. Por esse motivo não podem ser realizados em um reticulado quadrado, pois anéis de inteiros diferentes dos anéis de inteiros Gaussianos correspondem a reticulados diferentes, como por exemplo reticulados hexagonais no caso dos anéis de inteiros de Eisenstein - Jacobi. Entretanto, isso não impede de conseguirmos uma matriz do tipo A com determinante m e assim realizar o código.

Exemplo 5.9 *Veja que $m=7$ pode ser obtido da forma quadrática $x_1^2+3x_2^2$, ou ainda, um elemento ς com norma $N(\varsigma)=7$ pertencente ao anel de inteiros de Eisenstein - Jacobi, $\mathbb{Z}[\omega]$, cuja norma é dada por $N(\varsigma)=x^2+xy+y^2$, para $\varsigma=x+y\cdot\omega$, onde $\omega=\frac{1+i\sqrt{3}}{2}$. Este é um caso onde não podemos aplicar o método algébrico. No entanto, a matriz $A=\begin{bmatrix} 2 & 1 \\ -1 & 3 \end{bmatrix}$ que tem $detA=7$ nos fornece os vetores reticulados $(0,0),(2,1),(4,2),(6,3),(1,4),(3,5),(5,6)$ que definirão uma tesselação por poliminós. Tais poliminós podem ser formados pela junção de um quadrado 1×1 e um retângulo 2×3. Assim obtemos um código $[[14,2,3]]$, Figura 5.6.*

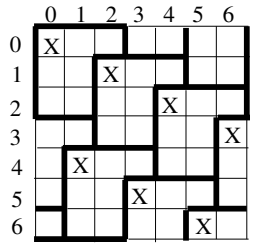

Figura 5.6: Código $[[14,2,3]]$.

Nos casos onde $m=p$ é um primo ímpar do tipo $p=4\kappa+3$, o conjunto dos representantes obtidos através desse método combinatorial, possui apenas um único X em cada linha ou coluna, portanto é um

código perfeito no sentido de [21], e a distância mínima do código decorrente desse processo coincide com a distância de Mannhein.

Na verdade, essa abordagem combinatorial é bastante ampla e pouco se pode fazer para tentar analisá-la por inteiro. São problemas combinatoriais apresentando dificuldades em decidir quais os possíveis valores para a, b, c e d, qual a melhor distribuição dos representantes ou ainda quais os melhores poliminós a serem usados. As duas últimas respostas só podem ser dadas de acordo com o tipo de canal sendo considerado.

Capítulo 6

Códigos TQC em Superfícies Compactas com $g \geq 2$

É possível generalizar a construção de códigos quânticos topológicos (TQC) para superfícies com gênero $g \geq 2$, [48]. No entanto, essa generalização, quando feita na literatura, é definida sobre mergulhos de células de grafos em superfícies, [12]. Esse modelo de construção não deixa claro o tipo de tesselação usada e nem quais os códigos possíveis de serem gerados. Nossa proposta de construção de tais códigos segue exatamente os mesmos passos da construção de Kitaev, levando em consideração a geometria associada às superfícies. Além disso, é possível exibir todos os possíveis códigos para cada superfície. Para simplificar o texto, a menos de menção contrária, escreveremos superfície para indicar uma superfície compacta orientável.

Uma das principais motivações para desenvolver esse trabalho se deve aos resultados obtidos em [16, 17, 71] que mostram que o desempenho, medido em termos de probabilidade de erro, de um sistema de comunicações utilizando constelações de sinais (modulação digital) em espaços com curvatura negativa $K < 0$, ou equivalentemente, em variedades bidimensionais com gênero $g \geq 2$ implicando na característica de Euler negativa, é melhor do que em espaços com curvatura $K \geq 0$. Como a modulação digital pode ser vista como uma classe de códigos, então conjectura-se de que os códigos corretores de erros mais eficientes oriundos de variedades bidimensionais com gênero $g \geq 2$ possam ser construídos.

Na Seção 6.1 fazemos uma breve revisão de geometria hiperbólica, visto que essa é a geometria associada às superfícies com gênero $g \geq 2$. Na Seção 6.2 mostramos como obter um modelo planar da superfície e apresentamos o modelo que será usado na construção sendo proposta. A Seção 6.3 mostra como determinar as tesselações do modelo planar. Na Seção 6.4 apresentamos a construção dos novos códigos, e as tabelas de todos os possíveis códigos gerados em superfícies com gênero $g = 2, 3, 4, 5$. A

Seção 6.5 mostra que a construção em consideração reproduz o código tórico de Kitaev e uma classe de códigos obtidos a partir de mergulhos auto-duais de grafos completos em superfícies apresentada em [13]. Além disso, ampliamos essa classe de códigos.

6.1 Geometria Hiperbólica

Em superfícies com gênero $g \geq 2$, a geometria a ser considerada é a *geometria hiperbólica*. A diferença entre a geometria hiperbólica e a geometria Euclidiana é que a primeira deixa de satisfazer o quinto postulado de Euclides, o axioma do paralelismo. Nesta seção revisamos alguns conceitos básicos de geometria hiperbólica necessários para o desenvolvimento desse trabalho. Para uma revisão mais aprofundada desse assunto sugerimos as referências [46, 8, 80].

Consideramos dois modelos de geometria hiperbólica: o *semi-plano superior*, $\mathbb{H}^2 = \{z = x+iy \in \mathbb{C} \mid Im(z) > 0\}$, e o *disco de Poincaré*, $\mathbb{D}^2 = \{z \in \mathbb{C} \mid |z| < 1\}$.

O espaço $\mathbb{H}^2$ munido da métrica

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y} \tag{6.1}$$

é conhecido como *plano hiperbólico* ou *plano de Lobachevski*. E essa métrica é chamada *métrica hiperbólica*.

A partir da equação (6.1), é possível definir os conceitos de comprimento hiperbólico e distância hiperbólica.

Definição 14 *Seja $\sigma : [a,b] \to \mathbb{H}^2$ um caminho diferenciável por partes, $\sigma(t) = \{z(t) = x(t) + iy(t) \in \mathbb{H}^2 | t \in [a,b]\}$. Então o comprimento hiperbólico de σ é definido por*

$$h(\sigma) = \int_\sigma \frac{\sqrt{(\frac{dx}{dt})^2 + (\frac{dy}{dt})^2}}{y(t)} dt = \int_a^b \frac{|\frac{dz}{dt}|}{y(t)} dt \tag{6.2}$$

Definição 15 *A distância hiperbólica entre dois pontos quaisquer $z, w \in \mathbb{H}^2$ é dada por*

$$d(z,w) = inf(h(\sigma)), \tag{6.3}$$

onde o ínfimo é considerado sobre o conjunto dos caminhos σ ligando z a w em $\mathbb{H}^2$.

Em [46] mostra-se que d é de fato uma métrica.

Considere a aplicação $f : \mathbb{H}^2 \to \mathbb{D}^2$ dada por

$$f(z) = \frac{zi+1}{z+i}, \tag{6.4}$$

Observa-se que f é uma aplicação injetiva, e que d^* dado por

$$d^*(z,w) = d(f^{-1}(z), f^{-1}(w)) \ \ (z,w \in \mathbb{D}^2) \tag{6.5}$$

é uma métrica em $\mathbb{D}^2$, e pode ser identificada com a métrica derivada da diferencial $ds = \frac{2|dz|}{1-|z|^2}$. Com essa convenção, f é uma isometria de $(\mathbb{H}^2, d)$ em $(\mathbb{D}^2, d)$. Isso nos permite trabalhar com o modelo mais adequado de acordo com a necessidade. A vantagem do modelo do disco de Poincaré é que por este ser um subconjunto limitado do plano Euclidiano, é mais conveniente para a visualização do plano hiperbólico. Por outro lado, o modelo do semi-plano superior nos permite usar coordenadas cartesianas nos cálculos.

A fronteira de $\mathbb{H}^2$, é dado por $\partial\mathbb{H}^2 = \mathbb{R} \cup \{\infty\}$, e é caracterizado pela propriedade da distância hiperbólica desses pontos a qualquer ponto no plano hiperbólico ser infinita, por isso o conjunto desses pontos é chamado *pontos no infinito* ou *círculo no infinito*. Já a fronteira de $\mathbb{D}^2$ é $\partial\mathbb{D}^2 = \{z \in \mathbb{C} : |z| = 1\}$ chamado *círculo principal* ou também *círculo no infinito*.

Geodésicas são caminhos com o menor comprimento hiperbólico ligando dois pontos distintos. Em $\mathbb{H}^2$ as geodésicas são semi-círculos e semi-retas ortogonais ao eixo real $\mathbb{R} = \{z \in \mathbb{C} \mid Im(z) = 0\}$. Enquanto as geodésicas em $\mathbb{D}^2$ são segmentos de círculos Euclidianos ortogonais a $\partial\mathbb{D}^2$, em particular seus diâmetros. Quaisquer dois pontos $z, w \in \mathbb{H}^2$ podem ser ligados por uma única geodésica, e a distância hiperbólica entre estes pontos é igual ao comprimento hiperbólico do único segmento de geodésica que os liga, [46].

Uma propriedade que diferencia a geometria hiperbólica da Euclidiana é que dado uma geodésica L e um ponto $z \in \mathbb{H}^2$ não pertencente a L , existe mais de uma geodésica passando por z que não intersecta L. Ou seja, $\mathbb{H}^2$, de fato, não satisfaz o quinto postulado de Euclides.

Seja $A \subset \mathbb{H}^2$, a *área hiperbólica* de A é dada por

$$\mu(A) = \iint_A \frac{dx\, dy}{y^2} \tag{6.6}$$

se essa integral existir.

No entanto, para determinar a área de um triângulo hiperbólico podemos usar o teorema de Gauss-Bonnet que mostra que a área hiperbólica de um triângulo hiperbólico depende apenas de seus ângulos. Lembramos que o *ângulo hiperbólico* entre duas geodésicas em $\mathbb{H}^2$ com intersecção no ponto z é o ângulo (Euclidiano) entre os vetores tangentes às geodésicas, e a soma dos ângulos internos de um triângulo hiperbólico é menor que π.

Teorema 1 *(Gauss-Bonnet) Seja Δ um triângulo hiperbólico com ângulos internos α, β, θ. Então a*

área de Δ *é dada por*

$$\mu(\Delta) = \pi - \alpha - \beta - \theta.$$

Os próximos conceitos são necessários para a definição de um grupo Fuchsiano, que por sua vez é importante devido ao fato do emparelhamento de lados de um polígono hiperbólico (modelo planar de superfícies, que veremos na Seção 6.2) ser realizado pelos elementos de um tal grupo.

Considere o grupo multiplicativo das matrizes reais 2×2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

com $a,b,c,d \in \mathbb{R}$ e $det(A) = 1$. Esse grupo é conhecido como *grupo unimodular* e é denotado por $SL(2,\mathbb{R})$.

Uma *transformação de Möbius* é uma aplicação $T : \mathbb{C} \to \mathbb{C}$ definida por

$$T(z) = \frac{az+b}{cz+d},$$

onde $a,b,c,d \in \mathbb{R}$ tal que $ad - bc = 1$. Podemos representar uma transformação de Möbius por matrizes do tipo $\pm A$, onde $A \in SL(2,\mathbb{R})$. Assim, a composição de duas transformações corresponde ao produto de duas matrizes, a transformação identidade corresponde a matriz identidade I_2, e a transformação inversa à matriz inversa. O *grupo projetivo especial linear*, denotado por $PSL(2,\mathbb{R})$, é o grupo multiplicativo de transformações de Möbius, equivalentemente, $PSL(2,\mathbb{R}) \cong SL(2,\mathbb{R}/\langle \pm I_2 \rangle$.

As transformações de Möbius dividem-se em três classes distintas: *elíptica*, *parabólica* e *hiperbólica*. A classificação destas transformações depende da *função traço de* T definida por $Tr(T) = [tr(A)]^2 = [tr(-A)]^2$, onde T é uma transformação de Möbius correspondente ao par de matrizes $\pm A \in SL(2,\mathbb{R})$ e $tr(A)$ é a função traço usual de matrizes. Pode-se verificar que essa função é bem definida. Assim, para $T \in PSL(2,\mathbb{R}) \setminus I_2$, tem-se que:

(i) T é elíptica se, e somente se, $Tr(T) < 4$;

(ii) T é parabólica se, e somente se, $Tr(T) = 4$;

(iii) T é hiperbólica se, e somente se, $Tr(T) > 4$.

Outra maneira de classificar as transformações de Möbius é através dos pontos fixados pela transformação. Seja T uma transformação de Möbius, dizemos que

(i) T é elíptica se tem um ponto fixo em $\mathbb{H}^2$ e nenhum em $\partial\mathbb{H}^2$;

(ii) T é parabólica se tem um ponto fixo em $\partial\mathbb{H}^2$ e nenhum em $\mathbb{H}^2$;

(iii) T é hiperbólica se tem dois pontos fixos em $\partial\mathbb{H}^2$ e nenhum em $\mathbb{H}^2$.

Se T fixa três ou mais pontos, então T é a identidade, e portanto fixa todo ponto.

As transformações de Möbius são homeomorfismos e preservam a distância hiperbólica em $\mathbb{H}^2$. Assim, o grupo $PSL(2,\mathbb{R})$ é um subgrupo do grupo de todas as isometrias de $\mathbb{H}^2$, denotado por $Isom(\mathbb{H}^2)$. Consequentemente, qualquer transformação em $PSL(2,\mathbb{R})$ leva geodésica em geodésica. Outro fato importante é que transformações de Möbius são *transformações conformes*, ou seja, preservam ângulos. Disso segue que a área hiperbólica é invariante sob todas as transformações em $PSL(2,\mathbb{R})$.

O grupo $PSL(2,\mathbb{R})$ pode ser visto como um espaço topológico em que cada transformação $T \in PSL(2,\mathbb{R})$, $T(z) = \frac{az+b}{cz+d}$, é identificada com o ponto $(a,b,c,d) \in \mathbb{R}^4$. Assim, como um espaço topológico, podemos identificar $SL(2,\mathbb{R})$ com o subconjunto de $\mathbb{R}^4$, $X = \{(a,b,c,d) \in \mathbb{R}^4 | ad-bc = 1\}$. Definindo a aplicação $\delta : X \to X$ por $\delta(a,b,c,d) = (-a,-b,-c,-d)$, vemos que δ é um homeomorfismo e além disso, δ junto com a identidade formam um grupo cíclico de ordem dois agindo em X.

A topologia em $PSL(2,\mathbb{R})$ é definida como o espaço quociente

$$PSL(2,\mathbb{R}) \simeq \frac{SL(2,\mathbb{R})}{\{\pm\delta\}},$$

onde a norma em $PSL(2,\mathbb{R})$ é induzida do $\mathbb{R}^4$: para cada $T \in PSL(2,\mathbb{R})$, $T(z) = \frac{az+b}{cz+d}$, com $ad-bc = 1$, definimos

$$\|T\| = (a^2+b^2+c^2+d^2)^{\frac{1}{2}}.$$

T está bem definida. Portanto, $PSL(2,\mathbb{R})$ é um espaço topológico com respeito à métrica $\|T-S\|$. Similarmente, o grupo $Isom(\mathbb{H}^2)$ é também um espaço topológico.

Definição 16 *Um subgrupo $\Gamma \subset Isom(\mathbb{H}^2)$ é discreto se a topologia induzida em Γ é uma topologia discreta, isto é, se Γ é um conjunto discreto no espaço topológico $Isom(\mathbb{H}^2)$.*

Definição 17 *Um grupo Fuchsiano é um subgrupo discreto de $PSL(2,\mathbb{R})$.*

Uma família $\{M_\alpha \mid \alpha \in \Omega\}$ de subconjuntos de X indexados por elementos de um conjunto Ω é chamada localmente finita se para qualquer subconjunto compacto $K \subset X$, $M_\alpha \cap K \neq \emptyset$ para apenas uma quantidade finita de $\alpha \in \Omega$. Considere um espaço métrico X e um grupo G de homeomorfismos de X. Dizemos que um grupo G age propriamente descontinuamente em X se a G-órbita de qualquer ponto $x \in X$, $G(x) = \{T(x) : T \in G\}$, é localmente finita. Assim, grupos Fuchsianos são caracterizados no seguinte teorema.

Teorema 2 [46] $\Gamma \subset PSL(2,\mathbb{R})$ *é um grupo Fuchsiano se, e somente se,* Γ *age propriamente descontinuamente em* $\mathbb{H}^2$.

Definição 18 *Seja* X *um espaço métrico e* Γ *um grupo de homeomorfismos agindo propriamente descontinuamente em* X. *Um subconjunto fechado* $\widetilde{F} \subset X$ *com interior não vazio é chamado região fundamental de* Γ *se*

(i) $\bigcup_{T\in\Gamma} T(\widetilde{F}) = X,$

(ii) $int\widetilde{F} \bigcap T(int\widetilde{F}) = \emptyset, \quad \forall\, T \in \Gamma - \{Id\},$

onde $int\widetilde{F}$ *é o conjunto de pontos interiores de* $\widetilde{F}$.

A família $\{T(\widetilde{F}) : T \in \Gamma\}$ é chamada *tesselação* de X.

A área de uma região fundamental, se finita, é um invariante numérico do grupo.

Seja Γ um grupo Fuchsiano e $z_1 \in \mathbb{H}^2$ tal que $T(z_1) \neq z_1$ para todo $T \in \Gamma \setminus \{id\}$, então $D_{z_1}(\Gamma) = \{z \in \mathbb{H}^2 \mid d(z,z_1) \leq d(z,T(z_1)),\ \forall\, T \in \Gamma\}$ é uma região fundamental de Γ, chamada *região de Dirichlet*.

6.2 Modelo Planar de uma Superfície

Para generalizar a construção de Kitaev dos códigos tóricos em superfícies compactas com gênero $g \geq 2$, precisamos primeiro selecionar um polígono hiperbólico P' que irá funcionar como o modelo planar da superfície, e depois precisamos determinar suas possíveis tesselações $\{p,q\}$. Nesta seção trataremos do problema de escolher o modelo planar da superfície.

Antes porém, se faz necessário uma breve revisão de alguns conceitos básicos de topologia de superfícies. Para uma revisão mais aprofundada desse assunto sugerimos as referências [77, 29].

Um *polígono hiperbólico* P' *com* p' *lados*, ou um p'-gon, é um conjunto convexo fechado consistindo de p' segmentos de geodésicas hiperbólicas. A intersecção de duas geodésicas é chamada *vértice* do polígono. Um p'-gon cujos lados têm o mesmo comprimento e os ângulos internos são iguais, é chamado um p'*-gon regular*.

Uma *tesselação regular* do plano Euclidiano ou hiperbólico, é uma cobertura de todo o plano por polígonos regulares, todos com o mesmo número de lados, sem superposições de tais polígonos, encontrando-se somente ao longo de arestas completas ou em vértices. Denotamos uma tesselação regular por $\{p,q\}$, onde q polígonos regulares com p lados encontram-se em cada vértice. Em particular, se $p = q$ a tesselação é dita *auto-dual*.

Considere uma tesselação regular $\{p,q\}$. Podemos observar que o ângulo interno de um p-gon em um vértice deve ser $\frac{2\pi}{q}$, e se considerarmos o polígono dividido em p triângulos, então o ângulo que está no centro do polígono será $\frac{2\pi}{p}$, enquanto os demais serão $\frac{2\pi}{2q}$. Portanto, no caso Euclidiano, temos que

$$\frac{2\pi}{p}+\frac{2\pi}{q}=\pi.$$

Segue-se que,

$$\begin{aligned} pq-2p-2q&=0\\ (p-2)(q-2)&=4. \end{aligned} \tag{6.7}$$

Para esta equação existem três soluções reais, ou seja, existem três tesselações regulares no plano Euclidiano. A saber, tesselações formadas por quadrados $\{4,4\}$, por hexágonos regulares $\{6,3\}$ e por triângulos equiláteros $\{3,6\}$.

No plano hiperbólico temos a seguinte relação:

$$\pi>\frac{2\pi}{q}+\frac{2\pi}{p}.$$

Então,

$$\begin{aligned} pq-2p-2q&>0\\ (p-2)(q-2)&>4. \end{aligned} \tag{6.8}$$

Existem infinitas soluções para esta inequação. Portanto, existem infinitas tesselações regulares no plano hiperbólico. Por exemplo, se $p=q$, então temos todas as tesselações auto-duais $\{p,p\}$, com $p>4$.

Gostaríamos de chamar atenção para a notação. O polígono regular hiperbólico que servirá de modelo planar da superfície, e que será denotado por P', é o polígono associado com a região fundamental da tesselação $\{p',q'\}$, ou seja, P' é um polígono com p' lados onde q' polígonos com p' arestas encontram-se em cada vértice. Enquanto a tesselação $\{p,q\}$ dentro de P' tem como região fundamental um polígono hiperbólico regular, denotado por P, com p lados onde q polígonos com p lados se encontram em cada vértice. A área desses dois polígonos estão relacionadas pela equação (6.13).

Um importante invariante topológico que usaremos nessa seção é a *característica de Euler*. Dada um região compacta X, podemos tesselar essa região com um número finito de cópias de um dado polígono. A característica de Euler de X, denotada por $\chi(X)$, é dada por

$$\chi(X)=V-E+F, \tag{6.9}$$

onde V denota o número de vértices dessa tesselação, E denota o número de arestas e F denota o número de faces (ou seja, o número de polígonos). Outra maneira de estabelecer a característica de Euler é através do gênero g de X, e então $\chi(X)$ é dada por

$$\chi(X) = 2 - 2g. \tag{6.10}$$

Note que, no caso de uma tesselação regular, se contarmos as q arestas em cada um dos V vértices, teremos contado cada aresta da tesselação duas vezes. Analogamente, se contarmos todas as p arestas correspondendo ao bordo de cada uma das F faces da tesselação, teremos contado cada aresta da tesselação duas vezes. Portanto, a seguintes igualdades são satisfeitas,

$$qV = 2E = pF. \tag{6.11}$$

Por exemplo, se considerarmos uma única face da tesselação, ou seja, um polígono P com p lados, então $F = 1, V = p/q$ e $E = p/2$.

6.2.1 Geração de uma superfície a partir de um polígono P'

Uma superfície topológica compacta $\mathbb{M}$ pode ser obtida de um polígono P' por pares de arestas (ou lados) identificadas, uma vez que as condições de comprimento e ângulo sejam satisfeitas.

A operação de identificação de pares de lados de um polígono hiperbólico P' é formalmente definida como uma transformação de emparelhamento de lados. Desde que o comprimento dos lados sejam iguais, uma transformação de emparelhamento de lados é uma isometria $\gamma \neq Id$ de um grupo de isometrias que preserva orientação Γ, levando um lado s de P' a outro lado $\gamma(s) = s'$ de P'. E também, $\gamma^{-1} \in \Gamma \setminus \{Id\}$ leva $\gamma(s) = s'$ a s. Assim, dizemos que os lados s e s' são emparelhados. Se s é identificada com s', e s' é identificada com s'', então s é identificada com s''. Tal cadeia de identificação pode ocorrer também com vértices, e então chamamos um conjunto maximal $\{v_1, v_2, \ldots v_k\}$ de vértices identificados de um *ciclo de vértices*.

Mais especificamente, sejam Γ um grupo de isometrias que preserva orientação e D um polígono (ou uma região de Dirichlet) para Γ. Assumimos que todos os vértices de D estejam dentro de $\mathbb{H}^2$. Uma transformação de emparelhamento de lados é uma isometria que preserva orientação $\gamma \in \Gamma \setminus \{Id\}$ que identifica um lado $s \in D$ com outro lado $s' = \gamma(s) \in D$. Note que cada vértice $v \in D$ é aplicado a outro vértice de D sob uma transformação de emparelhamento de lados associado a um lado cuja extremidade é v. Cada vértice v de D tem dois lados s e $*s$ de D com extremidade v. Denotamos por (v,s) um vértice v e um lado s de D com extremidade v, e por $(v,*s)$ o par do vértice v e o outro lado $*s$ com extremidade v. Considere o seguinte procedimento:

- (i) Seja $v = v_0$ um vértice de D e seja s_0 um lado com uma extremidade em v_0. Seja γ_1 uma transformação de emparelhamento de lados associada ao lado s_0. Assim γ_1 leva s_0 a um outro lado s_1 de D.
- (ii) Sejam $s_1 = \gamma_1(s_0)$ e $v_1 = \gamma_1(v_0)$. Isso fornece um novo par (v_1, s_1).
- (iii) Agora considere o par $(v_1, *s_1)$. Esse é o par consistindo do vértice v_1 e o lado $*s_1$.
- (iv) Seja γ_2 a transformação de emparelhamento de lados associada ao lado $*s_1$. Então, $\gamma_2(*s_1)$ é um lado s_2 de D e $\gamma_2(v_1) = v_2$, um vértice de D.
- (v) Repita o processo acima indutivamente. Veja Figura 6.1.

Assim, obtemos uma sequência de pares de vértices e lados:

$$\begin{pmatrix} v_0 \\ s_0 \end{pmatrix} \to \begin{pmatrix} v_1 \\ s_1 \end{pmatrix} \to \begin{pmatrix} v_1 \\ *s_1 \end{pmatrix} \to \begin{pmatrix} v_2 \\ s_2 \end{pmatrix} \to \cdots \begin{pmatrix} v_i \\ s_i \end{pmatrix} \to \begin{pmatrix} v_i \\ *s_i \end{pmatrix} \to \begin{pmatrix} v_{i+1} \\ s_{i+1} \end{pmatrix} \to \cdots$$

Como existe um número finito de pares (v, s), esse processo de aplicação de uma transformação de emparelhamento de arestas seguida de uma aplicação $*$ deve eventualmente retornar ao par inicial (v_0, s_0). Seja $\lambda > 0$ o menor inteiro para o qual $(v_\lambda, *s_\lambda) = (v_0, s_0)$. A sequência de vértices $v_0 \to v_1 \to \cdots \to v_{\lambda-1}$ é o ciclo de vértices, e a transformação $\gamma_\lambda \gamma_{\lambda-1} \cdots \gamma_2 \gamma_1$ é chamada uma *transformação de ciclo elíptico*. Como a quantidade de pares de vértices e lados é finita, então existe apenas uma quantidade finita de ciclos de vértices e transformações de ciclos elípticos.

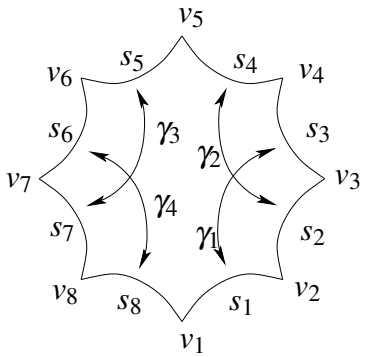

Figura 6.1: Exemplo de emparelhamento de lados de um octógono hiperbólico cujo ciclo elíptico é $\gamma_4^{-1}\gamma_3^{-1}\gamma_4\gamma_3\gamma_2^{-1}\gamma_1^{-1}\gamma_2\gamma_1$.

Um emparelhamento de lados de P' define um *espaço de identificação* $S_{P'}$. Esse espaço de identificação tem uma função distância que coincide com a distância hiperbólica para regiões suficientemente pequenas no interior de P', tornando-o uma superfície hiperbólica quando os ângulos de cada ciclo de vértices somam 2π.

Note que o número de lados de P' é par, uma vez que os lados são identificados aos pares. Poderia-se ter um número ímpar de lados, porém um lado teria que ser identificado consigo mesmo, adicionando um vértice no meio desse lado, mas esse não é o caso em consideração. Se P' é um 2-gon, então existem apenas duas possibilidades para a identificação de lados. Uma delas nos dá uma esfera e a outra o plano projetivo. Similarmente, se P' é um 4-gon, as possíveis identificações de lados resultam na esfera, plano projetivo, toro ou garrafa de Klein, e essas superfícies podem ser realizadas geometricamente como superfícies Euclidianas. Todas as outras superfícies compactas podem ser realizadas geometricamente como superfícies hiperbólicas.

Pode-se mostrar que qualquer superfície topológica $S_{P'}$ não homeomorfa a uma esfera é homeomorfa a uma superfície S_{P^*} para qual P^* tem um único ciclo de vértices. Assim, podemos assumir que P' tem um emparelhamento de lados particularmente simples. Portanto, qualquer superfície compacta pode ser realizada geometricamente, [77].

De acordo com o teorema de Killing-Hopf (veja Ref. [77]) qualquer superfície hiperbólica conexa completa é da forma $\mathbb{H}^2/\Gamma$, onde Γ age propriamente descontinuamente em $\mathbb{H}^2$, ou seja, Γ é um grupo Fuchsiano.

Do teorema de Killing-Hopf, desde que $S_{P'}$ é completo, ou seja, cada segmento geodésico em $S_{P'}$ pode ser estendido indefinidamente, podemos expressar $S_{P'}$ como um quociente $\mathbb{S}^2/\Gamma, \mathbb{R}^2/\Gamma$, ou $\mathbb{H}^2/\Gamma$. Pode-se mostrar que $S_{P'}$ é completo se P' é compacto, [77]. Assim, espaços de identificação de polígonos compactos podem ser realizados por superfícies geométricas.

Por outro lado, uma superfície compacta $\mathbb{S}^2/\Gamma, \mathbb{R}^2/\Gamma$, ou $\mathbb{H}^2/\Gamma$, é o espaço de identifica-ção de um polígono na geometria correspondente. A esférica ($\mathbb{S}^2/\Gamma$) e a Euclidiana ($\mathbb{R}^2/\Gamma$) são os casos mais simples entre os espaços de identificações.

As superfícies hiperbólicas $\mathbb{H}^2/\Gamma$ obtidas como espaços de identificação de polígonos são aquelas para as quais Γ é finitamente gerado. Como Γ é gerado por transformações de emparelhamento de lados e um polígono P' tem apenas uma quantidade finita de lados, então Γ é finitamente gerado se P' é uma região fundamental para Γ. A recíproca é verdade, basta construir uma região fundamental poligonal para um dado Γ finitamente gerado.

Assim, uma superfície hiperbólica compacta $\mathbb{H}^2/\Gamma$ é o espaço de identificação de um polígono se o polígono é uma região fundamental para Γ. Uma condição necessária e suficiente para um polígono ser uma região fundamental é a seguinte.

Condição de lado e ângulo [77]: *Se um polígono compacto P' é uma região fundamental para um grupo de isometrias que preservam orientação Γ de $\mathbb{S}^2$ (superfície esférica), $\mathbb{R}^2$ (plano Euclidiano),*

ou $\mathbb{H}^2$ (plano hiperbólico), então

(i) Para cada lado s de P' existe um único lado s' de P' tal que $s' = \gamma(s)$, para $\gamma \in \Gamma$;

(ii) Dado um emparelhamento de lados de P', para cada conjunto de vértices identificados, a soma dos ângulos tem que ser igual a 2π. Esse conjunto é um ciclo de vértices.

Teorema 8 (Poincaré) [77] *Um polígono compacto P' satisfazendo as condições de lado e ângulo é uma região fundamental para o grupo Γ gerado pelas transformações de emparelhamento de lados de P', e Γ é um grupo Fuchsiano.*

6.2.2 Classificação topológica de superfícies

Toda superfície geométrica é da forma $\mathbb{S}^2/\Gamma, \mathbb{R}^2/\Gamma$, ou $\mathbb{H}^2/\Gamma$, assim o problema de classificação de superfícies é trocado pelo problema de classificação dos grupos Γ. Uma maneira de distinguir superfícies hiperbólicas é usando topologia. Superfícies podem ser distinguidas topologicamente por seu gênero.

Como vimos, superfícies topológicas podem ser obtidas como o espaço de identificação $S_{P'}$ de um polígono P', e se P' não é homeomorfo a $\mathbb{S}^2$, então P' pode ser escolhido a ter um único ciclo de vértices. Usamos esse fato para classificar as superfícies não-esféricas $S_{P'}$ mostrando que todas tais superfícies são obtidas de polígonos cuja identificação de lados é dada na *forma normal*. As superfícies com diferentes formas normais são não-homeomorfas.

Denotamos as arestas identificadas no bordo de P' pela mesma letra, por exemplo a. Quando as arestas são diretamente opostas, denotamo-as por a, a^{-1}.

Na forma normal cada superfície compacta orientável é homeomorfa a um espaço de identificação $S_{P'}$ de um polígono P' com bordo da forma aa^{-1} or $a_1 b_1 a_1^{-1} b_1^{-1} \ldots a_g b_g a_g^{-1} b_g^{-1}$. No primeiro caso, $S_{P'}$ é dito ter gênero 0, no último caso $S_{P'}$ tem gênero g. O gênero g pode ser informalmente definido como o número de "alças" ou "buracos" porque cada segmento $a_i b_i a_i^{-1} b_i^{-1}$ no bordo de P' dá origem a uma alça. O gênero é o invariante que distingue topologicamente as superfícies. Uma construção mais detalhada da forma normal pode ser encontrada em [77].

Classificação geométrica das superfícies

Quando superfícies geometricamente orientáveis são construídas na forma normal, qualquer superfície de gênero 0 torna-se uma esfera (elíptica), qualquer superfície de gênero 1 torna-se um toro (Euclidiano), e superfícies com gênero ≥ 2 tornam-se um g-toro (hiperbólica). Reciprocamente, toda

superfície hiperbólica compacta orientável é de gênero ≥ 2, ou equivalentemente, sua característica de Euler é um número par negativo, devido a equação (6.10).

Seja $\mathbb{M} = \mathbb{H}^2/\Gamma$ uma superfície hiperbólica compacta. $\mathbb{M}$ pode ser realizada como o espaço de identificação $S_{P'}$ de um polígono convexo P' (a região de Dirichlet para o grupo Γ). A área desse polígono é uma propriedade geométrica que distingue tais superfícies. De fato, seja P' um polígono com p' arestas, ou um p'-gon, ou seja, a região fundamental da tesselação $\{p',q'\}$. Do teorema de Gauss-Bonnet, a área de $\mathbb{M}$ é dada por

$$\begin{aligned}
\mu(\mathbb{M}) &= \mu(P') \\
&= p'\left(\pi - \frac{2\pi}{p'} - \frac{2\pi}{q'}\right) \\
&= p'\left(\frac{\pi(p'q' - 2p' - 2q')}{p'q'}\right) \\
&= -2\pi\left(\frac{p'}{q'} - \frac{p'}{2} + 1\right) = -2\pi(V - E + F) \\
&= -2\pi\chi(S) = -2\pi(2-2g) \\
&= 4\pi(g-1), \qquad (6.12)
\end{aligned}$$

onde $V = p'/q'$ e $E = p'/2$.

6.2.3 Critério para escolha do polígono P'

Vimos que uma superfície compacta pode ser obtida de um polígono P' se este satisfaz a condição de lado e ângulo, e portanto o teorema de Poincaré, ou seja, P' é uma região fundamental para o grupo Fuchsiano Γ formado pelas transformações de emparelhamento de lados de P'.

Se P' é uma face da tesselação $\{p',q'\}$, podemos concluir que

- p' deve ser um inteiro par;
- considerando a característica de Euler da superfície (6.9) e (6.10) e as identificações de lados de P', temos que $V = \frac{p'}{q'}$, $E = \frac{p'}{2}$ e $F = 1$. Portanto, p' deve ser par e divisível por q'.

Assim, e lembrando que tesselações Euclidianas devem satisfazer (6.7) enquanto tesselações hiperbólicas devem satisfazer (6.8), concluímos que se q' for par, então $q' = 4,8,12,\ldots$, ou seja, $q' = 4r$, para $r = 1,2,3,\ldots$. Logo, p' deve ser da forma $(2r'-1)q'$, $r' = 1,2,3,\ldots$. E se q' for ímpar, então $q' = 2r+1$, e portanto $p' = 2(2r'-1)q'$, onde $r,r' = 1,2,3,\ldots$. Note que, para cada valor de q', variando o valor de r', obtemos um p' diferente. Mostramos alguns exemplos de possíveis tesselações cuja face gera uma superfície compacta na Tabela 6.1.

Pode-se classificar essas tesselações em função do gênero, como é visto na terceira coluna da Tabela 6.1, $\{4g,4g\}$, $\{4g+2,2g+1\}$, $\{8g-4,4\}$ e $\{12g-6,3\}$, entre outras. As tesselações auto-duais do tipo $\{4g,4g\}$, para o objetivo de gerar constelações de sinais geometricamente uniformes, são as tesselações menos densas, pois apresentam menos pontos no reticulado, consequentemente os pontos são mais distantes uns dos outros. As outras tesselações são usadas para obtenção de reticulados mais densos, dentre as quais a tesselação do tipo $\{12g-6,3\}$ é a mais densa, [79].

Tabela 6.1: Polígonos que geram superfícies compactas.

$\{p,q\}$	g	modelo da tesselação
$\{4,4\}$	1	$\{4g,4g\}$
$\{6,3\}$	1	$\{12g-6,3\}$
$\{8,8\}$	2	$\{4g,4g\}$
$\{10,5\}$	2	$\{4g+2,2g+1\}$
$\{12,4\}$	2	$\{8g-4,4\}$
$\{12,12\}$	3	$\{4g,4g\}$
$\{14,7\}$	3	$\{4g+2,2g+1\}$
$\{16,16\}$	4	$\{4g,4g\}$
$\{18,3\}$	2	$\{12g-6,3\}$
$\{18,9\}$	4	$\{4g+2,2g+1\}$
$\{20,4\}$	3	$\{8g-4,4\}$
$\{20,20\}$	5	$\{4g,4g\}$
$\{22,11\}$	5	$\{4g+2,2g+1\}$
$\{24,8\}$	5	$\{\frac{16g-8}{3},8\}$
$\{24,24\}$	6	$\{4g,4g\}$
$\{26,13\}$	6	$\{4g+2,2g+1\}$
$\{28,4\}$	4	$\{8g-4,4\}$
$\{28,28\}$	7	$\{4g,4g\}$
$\{30,3\}$	3	$\{12g-6,3\}$

Assim, para cada tipo de polígono proveniente de um dos modelos $\{4g,4g\}$, $\{4g+2,2g+1\}$, $\{8g-4,4\}$ e $\{12g-6,3\}$ é possível obter a superfície de gênero g de acordo com a transformação de emparelhamento de lados do polígono. Por exemplo, o grupo de Klein (veja Ref. [77]) é uma superfície de gênero 3 gerada a partir de um 14-gon que é uma face da tesselação $\{14,7\}$ ($\{4g+2,2g+1\}$) no plano hiperbólico, onde os lados são identificados pela relação $\gamma_i : s_{2i+1} \mapsto s_{2i+6}$, e a soma dos índices de s é realizada módulo 14, (Fig. 6.2). Note que, como esse 14-gon com a transformação de emparelhamento de lados dada, satisfaz o teorema de Poincaré, é uma região fundamental para Γ, onde Γ é o grupo consistindo das transformações de emparelhamento de lados. Neste exemplo, obtemos sete $(2g+1)$ transformações γ_i e dois ciclos de vértices cuja soma dos ângulos é igual a 2π. Quando mudamos o tipo de tesselação mudamos também as transformações de emparelhamento de lados, e

consequentemente o número dessas transformações e o número de ciclos de vértices. É claro que podemos ter para a mesma tesselação tipos diferentes de transformações que podem gerar a mesma superfície. Haja visto que a transformação na forma normal é sempre possível.

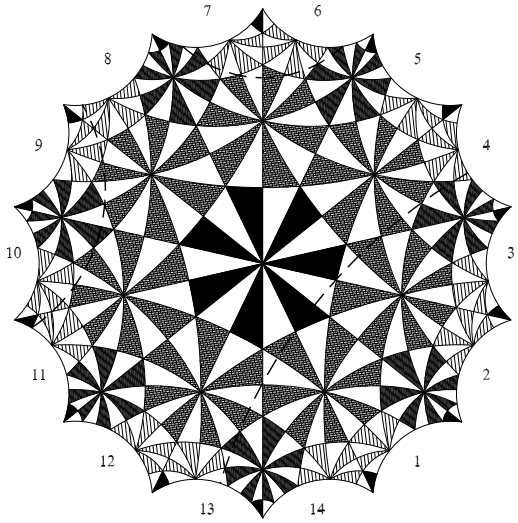

Figura 6.2: Grupo de Klein - um 14-gon com tesselação $\{7,3\}$ dentro.

Teoricamente, qualquer polígono que gere uma superfície compacta pode ser usado na construção de tais códigos. Porém, usaremos um critério para a escolha do nosso modelo planar de superfícies. Como foi visto no capítulo 3, a distância mínima de um código TQC está relacionada com os ciclos homologicamente não-triviais da superfície. Para que tenhamos a maior distância permitida, iremos considerar polígonos P' para os quais podemos identificar lados opostos. Isso é possível para polígonos $4g$-gon provenientes de tesselações do tipo $\{4g,4g\}$. De fato, considere $\gamma : S \to S$, dada por $\gamma(s_i) = s_{i+2g}$, onde $S = \{s_1,\ldots,s_{4g}\}$ é o conjunto de lados de P', $i = 1,2,\ldots,4g$, e a soma dos índices de s é realizada módulo $4g$. Tal isometria γ realiza o emparelhamento de lados opostos de P', veja Figura 6.3. Como $p' = q' = 4g$, o único ciclo de vértices obtido dessas transformações de emparelhamento de arestas tem a soma dos ângulos internos igual a $p'\frac{q'}{2\pi} = 2\pi$, portanto P' satisfaz o teorema de Poincaré. Note que, para esse modelo, existem $2g$ transformações e apenas um ciclo de vértices.

Nas referências [45, 53, 58] é possível observar que outros polígonos gerados a partir de tesselações mais densas não são capazes de satisfazer o teorema de Poincaré com transformações que emparelham lados opostos do polígono. Por esse motivo, nosso modelo planar será o polígono do tipo $4g$-gon.

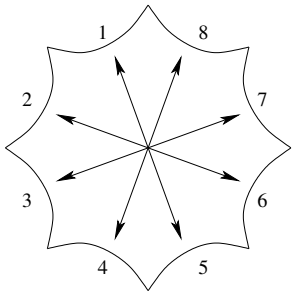

Figura 6.3: Transformação de emparelhamento de lados $\gamma(s_i) = s_{i+2g}$.

6.3 Tesselação $\{p,q\}$

Similarmente à construção de Kitaev, queremos determinar todas as possíveis tesselações $\{p,q\}$ do polígono P'. Para isso devemos determinar as soluções da equação

$$\mu(P') = n_f \mu(P), \tag{6.13}$$

onde as tesselações hiperbólicas devem satisfazer a seguinte desigualdade $(p-2)(q-2) > 4$. Na equação (6.13) $\mu(P')$ denota a área do polígono P' associado com a região fundamental da tesselação $\{p',q'\}$, $\mu(P)$ denota a área do polígono associado com a região fundamental da tesselação $\{p,q\}$, e n_f (número de faces da tesselação) é um inteiro positivo. Note que, dada uma tesselação $\{p,q\}$, a tesselação dual $\{q,p\}$ tem que satisfazer as mesmas condições anteriores.

As tesselações obtidas a partir da equação (6.13) satisfazem o Teorema 3 de Edmonds, Ewing e Kulkarni, [25]. Portanto, estas são de fato todas as possíveis tesselações de P'.

Teorema 3 [25] *Seja $\mathbb{M}$ uma superfície fechada e sejam p,q,V,E,F inteiros positivos tais que*

$$V - E + F = \chi(\mathbb{M}), \tag{6.14}$$

$$pF = 2E = qV. \tag{6.15}$$

Então os seguintes ítens são satisfeitos:

- *(Existência):Existe um $\{p,q\}$-padrão em $\mathbb{M}$ consistindo de F faces de p-lados, E arestas e V vértices cada um com valência q; exceto quando $\mathbb{M}$ é o plano projetivo, $\{p,q\} = \{3,3\}$, $V = F = 2$, e $E = 3$;*

- *(Geometrização): Um $\{p,q\}$-padrão em $\mathbb{M}$ pode ser realizado geometricamente;*

- *(Classificação): Um $\{p,q\}$-padrão na esfera ou no plano projetivo é único. Para todas as outras superfícies $\mathbb{M}$ os $\{p,q\}$-padrões em $\mathbb{M}$ são classificados por classes de conjugação de*

subgrupos isomorfos ao grupo fundamental de $\mathbb{M}$ *nos grupos de Schwarz estendidos* $(p,q,2)$*-triângulo.*

Como um exemplo, considere novamente o grupo de Klein. Ele é um 14-gon e pode ser tesselado com um conjunto de 24 heptágonos regulares idênticos, ou alternativamente, com um conjunto de 56 triângulos equiláteros. Essas duas tesselações são duais uma da outra, no sentido que os vértices de uma tesselação correspondem às faces da outra. Ou seja, o 14-gon é tesselado pela tesselação $\{7,3\}$ (veja Figura 6.2) e por sua tesselação dual $\{3,7\}$. Observe que a área do 14-gon é igual a área dos 24 heptágonos e a área dos 56 triângulos equiláteros.

Da equação (6.12) e do teorema de Gauss-Bonnet, a equação (6.13) pode ser escrita como:

$$4\pi(g-1) \quad = \quad n_f \left[(p-2)\pi - \frac{2p\pi}{q}) \right]. \tag{6.16}$$

Disso segue que o número de faces da tesselação $\{p,q\}$ de P' é dado por

$$n_f = \frac{4q(g-1)}{pq-2p-2q}. \tag{6.17}$$

A partir dessa equação (6.17), e lembrando que n_f deve ser um inteiro positivo, podemos explicitar todas as tesselações de P' atribuindo valores possíveis a p e q (veja Tabelas 6.2, 6.3, 6.4 e 6.5 como exemplos).

6.4 Construção de Códigos Quânticos Topológicos

Podemos definir formalmente um código quântico topológico da seguinte maneira.

Definição 19 *Seja* $\mathbb{M}$ *uma superfície compacta e* $\{p,q\}$ *uma tesselação de* $\mathbb{M}$ *com E arestas, V vértices e F faces. Dados um vértice* $v \in V$ *e uma face* $f \in F$*, definimos os operadores* A_v *como o produto tensorial de* σ_x *correspondendo a cada aresta tendo v como um vértice comum e os operadores* B_f *como o produto tensorial de* σ_z *correspondendo a cada aresta formando o bordo da face* f*. Um código quântico topológico* $\mathscr{C}$ *com comprimento* $n = |E|$*, com estabilizador* $\mathscr{S} = \{A_v |\ v \in V\} \cup \{B_f |\ f \in F\}$*, codifica* $k = 2g$ *qubits (se a superfície não tem bordo) e sua distância é* $d = min\{\delta, \delta^*\}$*, onde* δ *denota a distância do código na tesselação* $\{p,q\}$*, enquanto* δ^* *denota a distância código na tesselação dual* $\{q,p\}$*.*

Assim, para gerar os códigos TQC em superfícies com gênero $g \geq 2$, precisamos definir os operadores estabilizadores. Definidos esses operadores, podemos determinar os parâmetros do código.

6.4.1 Operadores e parâmetros

Como na construção de Kitaev, dado um vértice v da tesselação, o operador vértice age não trivialmente nos q qubits que têm o vértice v como extremidade, e nos qubits restantes age o operador identidade, isto é,

$$A_v = \bigotimes_{j \in E} \sigma_x^{\delta(j \in E_v)},$$

onde E_v denota o conjunto de arestas tendo v como um vértice comum.

Similarmente, dada uma face f da tesselação, o operador face age não trivialmente nos p qubits que formam o bordo desta face, e nos demais qubits da tesselação age a identidade, ou seja,

$$B_f = \bigotimes_{j \in E} \sigma_z^{\delta(j \in E_f)},$$

onde E_f denota o conjunto das arestas que formam o bordo de f. Portanto, o código é dado por

$$\mathscr{C} = \{|\psi\rangle : A_v|\psi\rangle = |\psi\rangle,\ B_f|\psi\rangle = |\psi\rangle \ \ \forall\ v, f\}.$$

Da equação (6.13), temos que n_f é o número de faces da tesselação $\{p', q'\}$ de P'. Como cada aresta desta tesselação pertence a duas faces simultaneamente, ao todo temos $n = n_f p/2$ arestas, ou qubits. Note que, n deve pertencer a $\mathbb{Z}^+$.

Os operadores A_v e B_f são os operadores estabilizadores deste código. Com efeito, A_v e B_f são operadores de Pauli e são mutuamente comutativos. Além disso, cada aresta é fronteira de duas faces ou tem dois vértices como extremidades, o que implica que cada aresta é contada duas vezes quando consideramos o produto de todos os operadores vértice ou face. Assim:

$$\prod_v A_v = 1 \quad \textit{and} \quad \prod_f B_f = 1. \tag{6.18}$$

Um operador vértice e um operador face podem ser expressos como o produto dos demais operadores do mesmo tipo. Conclui-se deste fato que existem $n_f - 1$ operadores face independentes e $n_v - 1$ operadores vértice independentes, onde n_v é o número de vértices da tesselação $\{p, q\}$ de P'. Assim, temos $n_f + n_v - 2$ geradores do grupo estabilizador. Consequentemente, o código deve codificar $k = n - (n_f + n_v - 2)$ qubits.

Note que, o número de vértices da tesselação coincide com o número de faces da tesselação dual, então $n_v = n_f p/q$. Da equação (6.16) temos

$$\begin{aligned} 2(2g-2) &= n_f p - 2n_f - 2n_f \frac{p}{q} \\ 2g-2 &= n_f \frac{p}{2} - n_f - n_f \frac{p}{q} \\ 2g-2 &= n - n_f - n_v \\ 2g &= n - n_f - n_v + 2. \end{aligned}$$

Portanto, o número de qubits codificados é $k = n - n_f - n_v + 2 = 2g$, e a dimensão do código $\mathscr{C}$ é $2^{2g} = 4^g$.

Substituindo o valor de n_f dado em (6.17), em $n = n_f \frac{p}{2}$, obtemos o valor de n em função de p, q e g. Então, para cada tesselação $\{p,q\}$, a taxa assintótica do código k/n é dada por $k/n \to \frac{pq-2p-2q}{pq}$ quando $g \to \infty$.

6.4.2 Distância do código

Lembramos que a distância de um código estabilizador é o peso do operador de Pauli de menor peso que preserva o subespaço do código e age não-trivialmente sobre o mesmo. Em termos de um código tórico, a distância é o mínimo entre o número de arestas contidas no menor ciclo homologicamente não-trivial da tesselação ou da tesselação dual, [22].

Para TQC em superfícies com gênero $g \geq 2$, a distância é similar à distância do código tórico. O que se deseja é procurar o menor ciclo homologicamente não-trivial da tesselação ou da tesselação dual. Tais ciclos em um p'-gon são dados pelas geodésicas de menor comprimento que ligam os lados identificados de P'. Em termos de arestas da tesselação de P', o menor ciclo homologicamente não-trivial é o caminho sobre as arestas que mais se aproxima das geodésicas de menor comprimento. Assim, a distância do código será o mínimo entre o número de arestas do menor ciclo homologicamente não-trivial da tesselação e da tesselação dual.

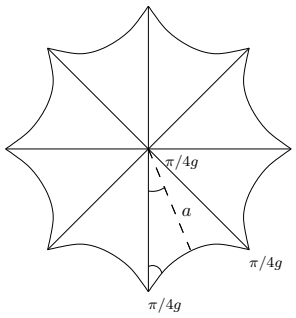

Figura 6.4: Comprimento hiperbólico $(2a)$ da menor geodésica ligando lados identificados de P'.

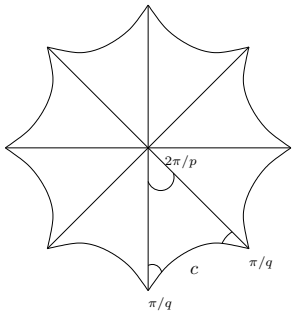

Figura 6.5: Comprimento da aresta (c) da tesselação $\{p,q\}$.

Com argumentos de trigonometria hiperbólica, é possível calcular facilmente a distância entre os lados emparelhados de P'. Esta distância, denotada por d_h, é o comprimento hiperbólico da geodésica ortogonal comum a estes dois lados, (Fig. 6.4), e é dada por

$$d_h = 2a = 2 \operatorname{arccosh}\left[\frac{\cos(\pi/4g)}{\operatorname{sen}(\pi/4g)}\right]. \tag{6.19}$$

Essa equação é obtida da relação $\cosh a \operatorname{sen}\beta = \cos\alpha$ (veja página 147 Ref. [8]), onde nesse caso $\alpha = \beta = \pi/4g$.

Como a distância do código, denotada aqui por d_{TQC}, deve ser dada em função das arestas da tesselação $\{p,q\}$ de P', obtemos um limitante inferior para tal distância dividindo o valor de d_h pelo comprimento da aresta, $l(p,q)$, da região fundamental da tesselação $\{p,q\}$, ou seja, $d_{TQC} \geq d_h/l(p,q)$, onde o comprimento da aresta da tesselação é dado por

$$l(p,q) \quad = \quad \operatorname{arccosh}\left[\frac{\cos^2(\pi/q)+\cos(2\pi/p)}{\operatorname{sen}^2(\pi/q)}\right]. \tag{6.20}$$

Essa expressão pode ser obtida pela regra do cosseno, $\cosh c = \frac{\cos\alpha\cos\beta+\cos\gamma}{\operatorname{sen}\alpha\operatorname{sen}\beta}$, onde c corresponde a aresta da tesselação $\{p,q\}$, (Fig. 6.5).

Assim, $d_{TQC} = \lceil \frac{d_h}{l(p,q)} \rceil$. Como os valores de $l(p,q)$ são invariantes, e d_h depende somente do gênero, segue que $d_h/l(p,q) \to \infty$ quando $g \to \infty$. Note que, $n = n_f \frac{p}{2} \to \infty$ quando $g \to \infty$. Contudo, a razão k/d_{TQC} não diverge necessariamente quando $g \to \infty$ devido ao valor de d_{TQC} crescer mais rapidamente do que k, e k não ser limitado.

6.4.3 Tabelas de códigos quânticos topológicos

O limitante inferior $d_h/l(p,q)$ da distância de um código definido sobre uma superfície compacta de gênero g depende da escolha da tesselação $\{p,q\}$ de P'. Quanto menor o comprimento hiperbólico da aresta da tesselação, maior será o limitante.

Da Equação (6.13) ou (6.17) podemos determinar todas as possíveis tesselações de $\{p,q\}$ de P'. Embora tenhamos uma extensiva lista de possíveis códigos, apresentamos nas Tabelas 6.2, 6.3, 6.4 e 6.5, os mais importantes códigos TQC em superfícies com gênero $2,3,4$ e 5, respectivamente. Os parâmetros considerados nessas tabelas são: a tesselação $\{p,q\}$ de P'; número de faces da tesselação, n_f; o comprimento da aresta da tesselação, $l(p,q)$; o limitante inferior da distância do código, $d_h/l(p,q)$; os parâmetros do código $[[n,k,d_{TQC}]]$, onde n denota o número de qubits, k denota o número de qubits codificados, e d_{TQC} é a distância mínima do código.

Note que, os maiores valores dos limitantes inferiores das distâncias estão associados às tesselações $\{3,7\}$ e $\{7,3\}$. Todavia, a distância mínima do código é o mínimo entre os valores $d_h/l(3,7)$ e $d_h/l(7,3)$. Consequentemente, a tesselação $\{3,7\}$ limitará a distância mínima do código resultante. Infelizmente, esse código tem taxa baixa. Por outro lado, a tesselação $\{4,5\}$ e sua tesselação dual $\{5,4\}$, em geral, têm a mesma distância enquanto mantém uma boa taxa. Como uma consequência, o código gerado pela tesselação $\{4,5\}$ e seu dual, é considerado o melhor código, pois em termos gerais, a tesselação $\{4,5\}$ mostra-se a melhor em relação a distância e taxa. As tesselações auto-duais apesar de apresentarem uma boa taxa, têm um dos menores valores para a distância. Por outro lado, os códigos definidos em tesselações auto-duais tem menor complexidade computacional. Uma possível aplicação para os códigos definidos em tesselações que não são auto-duais é que os mesmos podem ser usados quando há necessidade de proteção desigual.

A distância do código tórico cresce de acordo com o comprimento da aresta do toro plano, enquanto a distância em códigos de superfície com gênero $g \geq 2$ cresce em função do gênero da superfície.

Enfatizamos que a taxa assintótica do código é $k/n = \frac{pq-2p-2q}{pq}$ e $d_{TQC} \to \infty$ quando $g \to \infty$.

Na Tabela 6.6 fazemos uma comparação entre as taxas dos códigos com distância $d = 3,4$, e 5 para gênero $g = 1,2,3,4$, e 5. Observe que existem TQC cujas taxas de codificação são melhores que as do código tórico, quando a distância é fixada. Além disso, a taxa efetiva do código derivado das tesselações $\{4,5\}$ e $\{5,4\}$ quando $g = 2$, ou seja $[[20,4,3]]$, é a mesma taxa do código perfeito $[[5,1,3]]$ $(g = 0)$ e do código $[[10,2,3]]$ $(g = 1)$ obtido em [13].

Note que, existe TQC com distância $d = 5$ somente em superfícies com gênero $g \geq 4$. Além disso, códigos quânticos *MDS* com parâmetros $[[(2g+2),\ 2g,\ 2]]$, para $g = 2,3,4,5,...$, são mostrados em cada uma das tabelas. Todos os códigos apresentados nas Tabelas 6.2, 6.3, 6.4 e 6.5 respeitam o limitante quântico de Hamming, porém não o atinge.

O mais importante dessa construção é que com cálculos simples é possível explicitar todo código quântico topológico sobre uma superfície qualquer com gênero $g \geq 2$. A partir das tabelas de códigos

pode-se procurar por classes especiais de códigos.

Tabela 6.2: Tesselações e parâmetros dos TQC para $g = 2$ e $d_h = 3.0571$.

$\{p,q\}$	n_f	$l(p,q)$	$d_h/l(p,q)$	$[[n,k,d_{TQC}]]$
{3,7}	**28**	**1.0906**	**2.8033**	
{7,3}	**12**	**0.5663**	**5.3989**	**[[42,4,3]]**
{3,8}	16	1.5286	2	
{8,3}	6	0.7270	4.2049	[[24,4,2]]
{3,9}	12	1.8551	1.6480	
{9,3}	4	0.8192	3.7319	[[18,4,2]]
{3,10}	10	2.1226	1.4403	
{10,3}	3	0.8792	3.4773	[[15,4,2]]
{3,12}	8	2.5534	1.1973	
{12,3}	2	0.9516	3.2125	[[12,4,2]]
{4,5}	**10**	**1.2537**	**2.4384**	
{5,4}	**8**	**1.0613**	**2.8806**	**[[20,4,3]]**
{4,6}	6	1.7628	1.7343	
{6,4}	4	1.3170	2.3214	[[12,4,2]]
{4,8}	4	2.4485	1.2486	
{8,4}	2	1.5286	2	[[8,4,2]]
{5,5}	4	1.6850	1.8144	[[10,4,2]]
{6,6}	2	2.2924	1.3336	[[6,4,2]]

Tabela 6.3: Tesselações e parâmetros dos TQC para $g = 3$ e $d_h = 3.9833$.

$\{p,q\}$	n_f	$l(p,q)$	$d_h/l(p,q)$	$[[n,k,d_{TQC}]]$
{3,7}	**56**	**1.0906**	**3.6526**	
{7,3}	**24**	**0.5663**	**7.0347**	**[[84,6,4]]**
{3,8}	**32**	**1.5286**	**2.6059**	
{8,3}	**12**	**0.7270**	**5.4788**	**[[48,6,3]]**
{3,9}	**24**	**1.8551**	**2.1472**	
{9,3}	**8**	**0.8192**	**4.8625**	**[[36,6,3]]**
{3,10}	20	2.1226	1.8767	
{10,3}	6	0.8792	4.5307	[[30,6,2]]
{3,12}	16	2.5534	1.5600	
{12,3}	4	0.9516	4.1857	[[24,6,2]]
{3,14}	14	2.8982	1.3744	
{14,3}	3	0.9928	4.0123	[[21,6,2]]
{3,18}	12	3.4382	1.1585	
{18,3}	2	1.0359	3.8453	[[18,6,2]]
{4,5}	**20**	**1.2537**	**3.1771**	
{5,4}	**16**	**1.0613**	**3.7533**	**[[40,6,4]]**
{4,6}	**12**	**1.7628**	**2.2597**	
{6,4}	**8**	**1.3170**	**3.0246**	**[[24,6,3]]**
{4,8}	8	2.4485	1.6269	
{8,4}	4	1.5286	2.6059	[[16,6,2]]
{4,12}	6	3.3258	1.1977	
{12,4}	2	1.6629	2.3954	[[12,6,2]]
{5,5}	**8**	**1.6850**	**2.3640**	**[[20,6,3]]**
{5,6}	6	2.1226	1.8767	
{6,5}	5	1.8764	2.1228	[[15,6,2]]
{5,10}	4	3.2338	1.2318	
{10,5}	2	2.1226	1.8767	[[10,6,2]]
{6,6}	4	2.2924	1.7376	[[12,6,2]]
{6,9}	3	3.1614	1.2600	
{9,6}	2	2.4887	1.6006	[[9,6,2]]
{8,8}	2	3.0571	1.3030	[[8,6,2]]

Tabela 6.4: Tesselações e parâmetros dos TQC para $g = 4$ e $d_h = 4,596$.

$\{p,q\}$	n_f	$l(p,q)$	$d_h/l(p,q)$	$[[n,k,d_{TQC}]]$
{3,7}	**84**	**1.0906**	**4.2144**	
{7,3}	**36**	**0.5663**	**8.1165**	**[[126,8,5]]**
{3,8}	**48**	**1.5286**	**3.0067**	
{8,3}	**18**	**0.7270**	**6.3215**	**[[72,8,4]]**
{3,9}	**36**	**1.8551**	**2.4775**	
{9,3}	**12**	**0.8192**	**5.6104**	**[[54,8,3]]**
{3,10}	**30**	**2.1226**	**2.1653**	
{10,3}	**9**	**0.8792**	**5.2276**	**[[45,8,3]]**
{3,12}	24	2.5534	1.8000	
{12,3}	6	0.9516	4.8295	[[36,8,2]]
{3,15}	20	3.0486	1.5076	
{15,3}	4	1.0070	4.5639	[[30,8,2]]
{3,18}	18	3.4382	1.3367	
{18,3}	3	1.0359	4.4368	[[27,8,2]]
{3,24}	16	4.0374	1.1384	
{24,3}	2	1.0638	4.3204	[[24,8,2]]
{4,5}	**30**	**1.2537**	**3.6658**	
{5,4}	**24**	**1.0613**	**4.3306**	**[[60,8,4]]**
{4,6}	**18**	**1.7628**	**2.6073**	
{6,4}	**12**	**1.3170**	**3.4899**	**[[36,8,3]]**
{4,7}	**14**	**2.1408**	**2.1469**	
{7,4}	**8**	**1.4491**	**3.1717**	**[[28,8,3]]**
{4,8}	12	2.4485	1.8771	
{8,4}	6	1.5286	3.0067	[[24,8,2]]
{4,10}	10	2.9387	1.5640	
{10,4}	4	1.6169	2.8424	[[20,8,2]]
{4,12}	9	3.3258	1.3819	
{12,4}	3	1.6629	2.7639	[[18,8,2]]
{4,16}	8	3.9225	1.1717	
{16,4}	2	1.7073	2.6919	[[16,8,2]]
{5,5}	**12**	**1.6850**	**2.7277**	**[[30,8,3]]**
{5,10}	6	3.2338	1.4212	
{10,5}	3	2.1226	2.1653	[[15,8,2]]
{6,6}	**6**	**2.2924**	**2.0049**	**[[18,8,3]]**
{6,12}	4	3.7556	1.2238	
{12,6}	2	2.5534	1.8000	[[12,8,2]]
{8,8}	3	3.0571	1.5034	[[12,8,2]]
{10,10}	2	3.5796	1.2839	[[10,8,2]]

Tabela 6.5: Tesselações e parâmetros dos TQC para $g = 5$ e $d_h = 5,0591$.

$\{p,q\}$	n_f	$l(p,q)$	$d_h/l(p,q)$	$[[n,k,d_{TQC}]]$
{3,7}	**112**	**1.0906**	**4.6390**	
{7,3}	**48**	**0.5663**	**8.9343**	**[[168,10,5]]**
{3,8}	**64**	**1.5286**	**3.3097**	
{8,3}	**24**	**0.7270**	**6.9585**	**[[96,10,4]]**
{3,9}	**48**	**1.8551**	**2.7272**	
{9,3}	**16**	**0.8192**	**6.1757**	**[[72,10,3]]**
{3,10}	**40**	**2.1226**	**2.3835**	
{10,3}	**12**	**0.8792**	**5.7543**	**[[60,10,3]]**
{3,12}	32	2,5534	1.9813	
{12,3}	8	0.9516	5.3162	[[48,10,2]]
{3,14}	28	2.8982	1.7456	
{14,3}	6	0.9928	5.0959	[[42,10,2]]
{3,18}	24	3.4382	1.4714	
{18,3}	4	1.0359	4.8838	[[36,10,2]]
{3,22}	22	3.8576	1.3115	
{22,3}	3	1.0570	4.7861	[[33,10,2]]
{3,30}	20	4.4944	1.1257	
{30,3}	2	1.0765	4.6998	[[30,10,2]]
{3,54}	18	5.6828	0.8902	
{54,3}	1	1.0918	4.6336	[[27,10,2]]
{4,5}	**40**	**1.2537**	**4.0352**	
{5,4}	**32**	**1.0613**	**4.7670**	**[[80,10,5]]**
{4,6}	**24**	**1.7628**	**2.87**	
{6,4}	**16**	**1.3170**	**3.8415**	**[[48,10,3]]**
{4,8}	**16**	**2.4485**	**2.0662**	
{8,4}	**8**	**1.5286**	**3.3097**	**[[32,10,3]]**
{4,12}	12	3.3258	1.5212	
{12,4}	4	1.6629	3.0424	[[24,10,2]]
{4,20}	10	4.3785	1.1555	
{20,4}	2	1.7275	2.9286	[[20,10,2]]
{5,5}	**16**	**1.6850**	**3.0025**	**[[40,10,4]]**
{5,6}	**12**	**2.1226**	**2.3835**	
{6,5}	**10**	**1.8764**	**2.6961**	**[[30,10,3]]**
{5,10}	8	3.2338	1.5644	
{10,5}	4	2.1226	2.3835	[[20,10,2]]
{6,6}	**8**	**2.2924**	**2.2069**	**[[24,10,3]]**
{6,7}	7	2.6293	1.9241	
{7,6}	6	2.3884	2.1182	[[21,10,2]]
{6,9}	6	3.1614	1.6003	
{9,6}	4	2.4887	2.0328	[[18,10,2]]
{6,15}	5	4.2104	1.2016	
{15,6}	2	2.5827	1.9588	[[15,10,2]]
{7,14}	4	4.1520	1.2185	
{14,7}	2	2.8982	1.7456	[[14,10,2]]
{8,8}	4	3.0571	1.6548	[[16,10,2]]
{12,12}	2	3.9833	1.2701	[[12,10,2]]

Tabela 6.6: Códigos com distâncias $d = 3, 4$ e 5.

Distance	Genus	Tessellation	k/n
$d = 3$	1	$\{4,4\}$	$2/18$
		Ref. [13]	$2/10$
	2	$\{3,7\}$	$4/42$
		$\{4,5\}$	$4/20$
	3	$\{3,8\}$	$6/48$
		$\{3,9\}$	$6/36$
		$\{4,6\}$	$6/24$
		$\{5,5\}$	$6/20$
	4	$\{3,9\}$	$8/54$
		$\{3,10\}$	$8/45$
		$\{4,6\}$	$8/36$
		$\{4,7\}$	$8/28$
		$\{5,5\}$	$8/30$
		$\{6,6\}$	$8/18$
	5	$\{3,9\}$	$10/72$
		$\{3,10\}$	$10/60$
		$\{4,6\}$	$10/48$
		$\{4,8\}$	$10/32$
		$\{5,6\}$	$10/30$
		$\{6,6\}$	$10/24$
$d = 4$	1	$\{4,4\}$	$2/32$
		Ref. [13]	$2/17$
	3	$\{3,7\}$	$6/84$
		$\{4,5\}$	$6/40$
	4	$\{3,8\}$	$8/72$
		$\{4,5\}$	$8/60$
	5	$\{3,8\}$	$10/96$
		$\{5,5\}$	$10/40$
$d = 5$	1	$\{4,4\}$	$2/50$
		Ref. [13]	$2/26$
	4	$\{3,7\}$	$8/126$
	5	$\{3,7\}$	$10/168$
		$\{4,5\}$	$10/80$

6.5 Reprodução de Códigos Conhecidos

Com a construção proposta é possível reproduzir o código de Kitaev definido no toro, considerando a geometria Euclidiana. Também é possível reproduzir códigos em superfícies com gênero $g \geq 2$ obtidos em [13].

6.5.1 Código tórico de Kitaev revisitado

O código tórico pode ser obtido a partir da construção proposta neste trabalho. Para isso, basta considerar $g = 1$. Obviamente a determinação da área ocorre de maneira diferente e mais simples por se tratar do espaço Euclidiano.

Considere um reticulado quadrado $l \times l$ do toro, onde a aresta do reticulado é uma unidade de medida. Temos que, a área do polígono 4-gon que define o toro é $A = l^2$, enquanto a área da face da tesselação $\{4,4\}$ dentro do 4-gon é $A_i = 1$. Da equação (6.13), segue que $n_f = l^2$. Portanto, o número que qubits usados para codificar $2g = 2$ qubits é:

$$\begin{aligned} n &= n_f \frac{p}{2} \\ &= l^2 \frac{4}{2} \\ &= 2l^2 \end{aligned} \tag{6.21}$$

que coincide com o número de arestas obtido em [48].

Observe que o menor ciclo homologicamente não-trivial no reticulado quadrado do toro é exatamente a geodésica de menor comprimento entre lados identificados do quadrado que também coincidem com os eixos coordenados do toro plano. Assim, a distância é o comprimento do lado do polígono (quadrado), segue que $d = l$. Portanto, os parâmetros do código tórico são $[[2d^2, 2, d]]$.

6.5.2 Classe de códigos com distância 3 em superfícies com gênero $g \geq 2$

A construção proposta também reproduz os resultados mostrados em [13], ou seja, a família de códigos com parâmetros

$$\left[\left[\begin{pmatrix} s \\ 2 \end{pmatrix}, \begin{pmatrix} s \\ 2 \end{pmatrix} - 2(s-1), 3\right]\right],$$

quando consideramos o mergulho de grafos completos K_s, para $s \equiv 1 \ mod \ 4$, em superfícies com gênero apropriado.

Um grafo finito G consiste de um conjunto finito V_G de vértices, um conjunto finito E_G de arestas e uma função incidência I_G que associa a cada aresta e um conjunto de extremidades $V_G(e)$ contendo um ou dois elementos do conjunto de vértices V_G. Um grafo é chamado *simplicial* se ele não possui auto-malhas ou múltiplas arestas. Um grafo simplicial é chamado *completo* se todo par de vértices é adjacente, ou seja, eles são as extremidades da mesma aresta. Um grafo completo com s vértices é denotado por K_s.

Um grafo é dito *mergulhável* em uma superfície $\mathbb{M}$ se ele pode ser desenhado em $\mathbb{M}$ sem que exista cruzamento de arestas. O gênero de um grafo é o menor gênero de qualquer superfície na qual o grafo pode ser mergulhado, e é denotado por $\chi(G)$. O mergulho de um grafo é dito orientável se $\mathbb{M}$ é uma superfície orientável. Para maiores informações sobre grafos sugerimos a referência [42].

O dual de um mergulho de um grafo em uma superfície é obtido considerando o interior de cada face do mergulho original como um vértice de um novo grafo mergulhado. Se duas faces são adjacentes ao longo de uma aresta no grafo original, ligamos as duas faces (agora vértices do novo grafo) com uma nova aresta cruzando a aresta original ao longo da qual as duas faces são adjacentes. O mergulho resultante do novo grafo na mesma superfície é chamado o dual do mergulho original, e se o grafo dual é isomorfo ao original, então o mergulho original e o novo são ditos *auto-duais*.

Sejam V, E e F respectivamente o número de vértices, arestas e faces em um mergulho orientável auto-dual de K_s. Pode-se mostrar que se o mergulho é feito em uma superfície com gênero g, então

$$V = F = s, \quad E = \frac{s(s-1)}{2} = \left(\begin{array}{c} s \\ 2 \end{array} \right).$$

Assim, a característica de Euler desse grafo é dada por $\chi(K_s) = s - \frac{s.(s-1)}{2} + s$. Como $\chi(K_s) = \chi(\mathbb{M}) = 2-2g$, temos $g = \frac{(s-1)(s-4)}{4}$. Portanto, um tal mergulho pode existir somente se $s \equiv 0$ ou 1 *mod* 4, [60].

Portanto, quando consideramos códigos TQC, temos que $k = 2g = \left(\begin{array}{c} s \\ 2 \end{array} \right) - 2(s-1)$; o número de arestas do polígono resultante do mergulho do grafo completo K_s em uma superfície compacta com gênero g, é igual ao número de arestas do grafo. Logo, $n = \left(\begin{array}{c} s \\ 2 \end{array} \right)$. Logo, obtemos códigos quânticos topológicos com parâmetros

$$[n,\, k] = \left[\left(\begin{array}{c} s \\ 2 \end{array} \right),\, \left(\begin{array}{c} s \\ 2 \end{array} \right) - 2(s-1) \right].$$

Alguns exemplos são mostrados na Tabela 6.7, cuja distância mínima é d_{TQC}.

Da Tabela 6.7, note que a sequência em s dada por 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, $\cdots$ é a união de duas progressões aritméticas: $a_m = 4 + (m-1)4 = 4m$ e $b_m = 5 + (m-1)4 = 4m+1$, com $m \geq 1$.

Grafo K_s - s	Gênero - g	$[[n,k,d]]$
4	0	[[6, 0, 4]]
5	1	[[10, 2, 3]]
8	**7**	**[[28, 14, 3]]**
9	10	[[36, 20, 3]]
12	**22**	**[[66, 44, 3]]**
13	27	[[78, 54, 3]]
16	**45**	**[[120, 90, 3]]**
17	52	[[136, 104, 3]]

Tabela 6.7: Códigos quânticos topológicos derivados de mergulhos de grafos K_s em superfícies compactas.

A sequência b_m fornece os códigos topológicos propostos em [12], enquanto a sequência a_m, $m > 1$, gera uma nova classe de códigos quânticos topológicos, destacados em negrito na Tabela 6.7.

Para saber quais as tesselações que dão origem a esses códigos, observe que, em [13] temos

$$n = s(s-1)/2,$$

e segundo nossa construção $n = n_f p/2$. Então, tomando $n_f = s \equiv 1 mod 4$ e $p = n_f - 1 = s - 1$, e lembrando que $k = \begin{pmatrix} s \\ 2 \end{pmatrix} - 2(s-1) = 2g$, temos que:

$$\begin{aligned}
n_f &= \frac{4q(g-1)}{pq-2p-2q} \\
s &= \frac{4qg-4q}{pq-2p-2q} \\
s &= \frac{2q[\frac{s(s-1)}{2} - 2(s-1)] - 4q}{(s-1)q-2q-2(s-1)} \\
s(s-1)q - 2qs - 2s(s-1) &= s(s-1)q - 4q(s-1) - 4q \\
-2qs - 2s(s-1) &= -4q(s-1) - 4q \\
-2qs - 2s(s-1) &= -4qs \\
-2qs + 4qs - 2s(s-1) &= 0 \\
2qs &= 2s(s-1) \\
q &= s-1
\end{aligned} \tag{6.22}$$

Portanto, são tesselações auto-duais $\{s-1, s-1\}$. Veja alguns exemplos nas Tabelas 6.8 e 6.9

Tabela 6.8: Códigos derivados de mergulhos de grafos segundo a sequência a_m.

s	g	n_f	$\{p,q\}$	d_h	$l(p,q)$	$d_h/l(p,q)$	$[[n,k,d_TQC]]$
8	7	8	{7,7}	5,7465	2,7201	2,1126	[[28,14,3]]
12	22	12	{11,11}	8,05	3,7926	2,1226	[[66,44,3]]
16	45	16	{15,15}	9,4824	4,4604	2,1259	[[120,90,3]]
20	76	20	{19,19}	10,5308	4,9533	2,126	[[190,152,3]]

Tabela 6.9: Códigos derivados de mergulhos de grafos segundo a sequência b_m.

s	g	n_f	$\{p,q\}$	d_h	$l(p,q)$	$d_h/l(p,q)$	$[[n,k,d_TQC]]$
9	10	9	{8,8}	6,4674	3,0571	2,1155	[[36,20,3]]
13	27	13	{12,12}	8,4601	3,9833	2,1239	[[78,54,3]]
17	52	17	{16,16}	9,7716	4,596	2,1261	[[136,104,3]]
21	85	21	{20,20}	10,7546	5,0591	2,1258	[[210,170,3]]

Conclusões

O interesse em codificação quântica, com ênfase em códigos de superfícies, é o ponto de partida desse trabalho que pode ser dividido em dois resultados principais: a construção de novos códigos quânticos tóricos e a construção de códigos quânticos topológicos em superfícies compactas com gênero $g \geq 2$. Em ambas as construções obtemos importantes classes de códigos quânticos.

Em relação aos códigos quânticos tóricos, observou-se que seria possível ampliar seu estudo e, portanto, gerar muitos novos códigos desse tipo, se relacionássemos a eles conhecimentos de reticulados e formas quadráticas. Assim, através de uma abordagem algébrica e usando o conceito de poliminó, já usado para códigos clássicos, foi possível gerar um método de obtenção de códigos tóricos por meio da tesselação do reticulado quadrado do toro por translações desse poliminó. Códigos definidos dessa maneira mantém as mesmas propriedades dos códigos de Kitaev, como a localidade dos operadores estabilizadores, e continuam sendo definidos no reticulado $\mathbb{Z}^2$ que é ortogonal e auto-dual.

O modelo do poliminó usado na tesselação determina o padrão de correção de erros do código. Por exemplo, as esferas de Lee de raio r, na métrica de Lee, proporcionam códigos cujo padrão de correção de erros é simétrico, porém existem outros poliminós que podem ser utilizados para os casos onde o canal não seja simétrico. Assim, pode-se determinar o código que melhor se adapta ao problema.

Além de reproduzir classes de códigos já conhecidas, esse método permite encontrar outras classe de códigos tóricos, como por exemplo a classe $[[d^2, 2, d]]$ que é a melhor em termos de comprimento do código, e consequentemente a melhor quanto à taxa de codificação.

A segunda parte desse trabalho apresenta uma generalização da construção de códigos quânticos topológicos de gênero 1 para gêneros $g \geq 2$. Essa generalização segue naturalmente da geometria e da topologia associadas a essas superfícies. Os fundamentos dessa construção estão enraizados na estrutura geométrica relacionada as superfícies cujo gênero é $g \geq 2$, a saber a geometria hiperbólica, e nas conexões estabelecidas entre o modelo planar das superfícies compactas e suas tesselações. A partir da determinação do modelo planar da superfície e das tesselações possíveis para esse modelo,

tornou-se possível a caracterização dos códigos através dos operadores estabilizadores. Em particular, a determinação da distância como uma aproximação por meio de arestas do comprimento do menor ciclo homologicamente não-trivial, usando cálculos de trigonometria hiperbólica, mostrou ser a parte mais delicada da definição dos códigos, contudo constatou-se ser esta uma excelente aproximação. Enfatizamos que essa construção, apesar de usar conceitos de geometria hiperbólica e topologia de variedades bidimensionais, permite obter códigos realizando cálculos simples e rápidos.

Para uma melhor visualização, foi explicitado nas Tabelas 6.2, 6.3, 6.4 e 6.5 os códigos em superfícies compactas com gêneros $g = 2, 3, 4$ e 5, respectivamente, cujas distâncias são $d \geq 2$. Observando essas tabelas foi possível verificar que certas tesselações fornecem códigos com melhores parâmetros e taxas, ou seja, é possível encontrar classes de bons códigos. Em geral, a taxa de codificação converge para uma constante diferente de zero que depende apenas da tesselação selecionada. Além disso, a distância mínima do código cresce a medida que aumenta o gênero da superfície.

Dentre os códigos gerados no capítulo 6, encontramos uma classe de códigos MDS, além de reproduzir e ampliar a classe de códigos com distância 3 apresentada em [13]. Alguns desses códigos são explicitados nas Tabelas 6.8 e 6.9. A Tabela 6.6 mostra que ao se comparar os os códigos tóricos da literatura com os códigos das tabelas anteriores, a taxa desses últimos podem ser melhores quando a distância é fixada.

Outra observação pertinente aos códigos obtidos dessa construção, é que para tesselações que não são auto-duais os códigos gerados possuem proteção desigual inerente.

Partes desse trabalho foram apresentadas em congressos internacionais, a saber *IEEE Information Theory Workshop 2008* em Porto, Portugal, [2], e *Fifth International Conference of Applied Mathematics and Computing 2008*, em Plovdiv, Bulgária, [3], cujo artigo foi publicado na revista *International Journal of Pure and Applied Mathematics*, [5], revisada e indexada pela Mathematical Review e ZENTRALBLATT MATH. Além disso, referente à construção de códigos quânticos topológicos em superfícies compactas com gênero $g \geq 2$, foi publicado um artigo na revista *Journal of Mathematical Physics*, [4], que foi selecionado depois pelo *Virtual Journal of Quantum Information*. Atualmente aguardamos a resposta da revista *SIAM Journal on Discrete Mathematics* sobre o artigo relacionado à construção de novos códigos tóricos.

Sugestões para Futuras Pesquisas

Para dar prosseguimento a este trabalho, sugerimos os seguintes tópicos:

- Com respeito aos códigos quânticos tóricos, pode-se analisar algumas relações combinatoriais

no sentido de estabelecer melhor as condições para a geração de códigos dessa classe.

- Ainda dentro dessa classe de códigos, pode-se aprofundar o estudo de subclasses de códigos com melhores taxas e limitantes.

- Em relação aos códigos quânticos topológicos, muitas outras classes, como a classe de códigos com distância 3 decorrentes de tesselações auto-duais, podem ser encontradas e estudadas.

- A construção de classes de códigos em superfícies com gênero $g \geq 2$ similarmente à construção dos códigos tóricos usando poliminós.

- Avaliar as probabilidades de erros desses códigos.

- A construção de códigos quânticos topológicos em superfícies não-compactas com gênero $g \geq 2$ é uma outra possibilidade de estudo.

- Considerar a aplicação do método de construção de códigos quânticos topológicos em questões abertas no campo da correção de erro topológica, como a versão topológica do resultado sobre a existência de bons códigos quânticos em [15].

- O estudo de códigos topológicos para qubits $q = 2$ em superfícies não-orientáveis, e qudits com $q > 2$.

Comentário Final

É conhecido que a pesquisa em áreas de fronteira da ciência produzem conhecimento, tecnologia e crescimento para um país. A exemplo do que ocorre em outros países com estudos mais avançados em teoria de codificação quântica, a parceria entre matemática, física e teoria de informação e codificação, podem render bons resultados práticos. Uma boa base em matemática e em teoria de codificação podem auxiliar no entendimento de propriedades fundamentais para a construção de códigos quânticos e suas implementações.

Esta é a quarta tese de doutorado da Unicamp abordando temas relacionados à teoria de codificação quântica. Anteriormente, foram defendidas as teses sobre códigos convolucionais quânticos concatenados por Antônio Carlos Aido de Almeida, [6], sobre estudo de emaranhamento quântico com base em teoria da codificação clássica por Wanessa C. Gazzoni, [33], e sobre métodos de construção de códigos quânticos CSS e conexões entre códigos quânticos e matróides por Giuliano G. La Guardia

[49]. Espera-se que estes quatro trabalhos incentivem a pesquisa nessa área e proporcionem conhecimento e tecnologia para o país.

Bibliografia

[1] M. C. Abdalla e S. Kon. *O Discreto Charme das Partículas Elementares*. Unesp, São Paulo, (2006).

[2] C. D. de Albuquerque, R. Palazzo Jr. and E. B. da Silva, "Construction of topological quantum codes on compact surfaces, "in *Proceedings of the IEEE Information Theory Workshop*, Porto, Portugal, May 2008, pp. 391–395, (2008).

[3] C. D. de Albuquerque, R. Palazzo Jr. and E. B. da Silva, "On toric quantum codes, "in *Proceedings of the Fifth International Conference of Applied Mathematics and Computing*, Plovdiv, Bulgária, 2008. v. 1. p. 27, (2008).

[4] C. D. de Albuquerque, R. Palazzo Jr. and E. B. da Silva. "Topological quantum codes on compact surfaces with genus $g \geq 2$, " *Journal of Mathematical Physics* **50**, pp. 023513, (2009).

[5] C. D. de Albuquerque, R. Palazzo Jr. and E. B. da Silva. "On toric quantum codes, " *International Journal of Pure and Applied Mathematics*, **50**, pp. 221–226, (2009).

[6] A. C. A. Almeida. *Códigos Convolucionais Quânticos Concatenados*. Tese de doutorado, FEEC - UNICAMP, Campinas-SP, (2004).

[7] E. Artin and H. Braun. *Introduction to Algebraic Topology*. Charles E. Merrill Publishing Company, Columbus, Ohio, (1969).

[8] A. Beardon. *The Geometry of Discret Groups*. Springer-Verlag, New York, (1983).

[9] C. Bennett and G. Brassard. "Quantum cryptography: public key distribution and coin tossing, " *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984*, pp. 175–179, (1984).

[10] C. Bennett and S. Wiesner "Communication via 1-and 2-particle operators on Einstein-Podolsky-Rosen states, " *Phys. Rev. Lett.*, **69**, pp. 2881–2884, (1992).

[11] E. R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill Book Company, (1968).

[12] H. Bombin and M. A. Martin-Delgado. "Topological quantum error correction with optimal encoding rate, " *Physical Review A*, **73**, pp. 062303, (2006).

[13] H. Bombin and M. A. Martin-Delgado. "Homological error correction: classical and quantum codes, " *J. Math. Phys.*, **48**, pp. 052105, (2007).

[14] A. O. Caldeira. "Efeitos quânticos macroscópicos, dissipação quântica e qubits, " *Palestra para grupo temático Teoria da Informação e Códigos, N°* $2007/56052-8$ *(FAPESP)*, (2008).

[15] A. R. Calderbank and P. W. Shor. "Good quantum error-correcting codes exist, " *Physical Review A*, **54**, pp. 1098–1105, (1996).

[16] R. G. Cavalcante and R. Palazzo. "Análise de desempenho de constelações de sinais geometricamente uniformes provenientes de tesselações $\{p,q\}$ em espaços bidimensionais com curvatura constante, " *XXI Simpósio Brasileiro de Telecomunicações - SBT 04*, Belém-PA, (2004).

[17] R. G. Cavalcante, H. Lazari, J. D. Lima and R. Palazzo Jr. "A new approach to the design of digital communication systems, "*AMS - DIMACS Series*, vol. **68**, pp. 145-177 (2005).

[18] R. Cleve. "Quantum stabilizer codes and classical linear codes, " *www.arxiv.org/abs/quant-ph/9612048*, (1996).

[19] G. P. Collins. "Nós quânticos na computação, " *Scientific American Brasil*, **48**, pp. 49–55, (2006).

[20] J. H. Conway and N. J. A. Sloane. *Sphere Packings Lattices and Groups* Springer-Verlag, (1988).

[21] S. I. R. Costa, M. Muniz, E. Agustini and R. Palazzo Jr. "Graphs, Tessellations, and Perfect Codes on Flat Tori, " *IEEE Transactions on Information Theory*, Vol. 50, No. 10, October 2004.

[22] E. Dennis, A. Kitaev, A. Landahl and J. Preskill "Topological quantum memory, " *J. Mathematical Physics*, **43**, pp. 4452, (2002).

[23] D. Deutsch. “Quantum theory, the Church-Turing principle and the universal quantum computer, ” *Proc. R. Soc. Lond. A*, **400** pp.97, (1985).

[24] D. Deutsch and A. Ekert. “Quantum computation, ” *www.qubit.org*

[25] A. L. Edmonds, J. H. Ewing and R. S. Kulkarni. “Regular tesselations of surfaces and $(p,q,2)$-triangle groups, ” *Annals of Mathematics*, **116**, pp. 113–132, (1982).

[26] A. Einstein, B. Podolsky and N. Rosen. “Can quantum-mechanical description of physical reality be considered complete?, ” *Phys. Rev. Lett.*, **47**, pp.777, (1935).

[27] A. Ekert. “Quantum cryptography based on Bell’s theorem, ” *Phys. Rev. Lett.*, **67**, pp. 661, (1991).

[28] R. P. Feynman. “Simulating physics with computers, ” *Int. J. Theory Physics*, **21**, pp. 467, (1982).

[29] P. A. Firby and C. F. Gardiner. *Surface Topology*. Ellis Horwood Series in Mathematics and its Applications, England, (1991).

[30] M. H. Freedman, A. Kitaev and Z. Wang. “Simulation of topological field theories by quantum computers, ” *arXiv: quant-ph/0001071v3*, (2000).

[31] M. H. Freedman and D. A. Meyer. “Projective plane and planar quantum codes, ” *Found. Comput. Math.*, pp.325, (2001).

[32] E. F. Galvão. *O que é Computação Quântica?*. Vieira & Lent, Rio de Janeiro, Rio de Janeiro, (2007).

[33] W. C. Gazzoni. *Estudo do Emaranhamento Quântico com Base na Teoria da Codificação Clássica*. Tese de doutorado, FEEC - UNICAMP, Campinas-SP, (2008).

[34] P. J. Giblin. *Graphs, Surfaces and Homology*. A Halsted Press, (1977).

[35] R. Gilmore. *Alice no País do Quantum*. Jorge Zahar Editor Ltda, Rio de Janeiro, (1998).(Neste livro os conceitos da mecânica quântica são apresentados em uma linguagem bastante acessível e ilustrados com exemplos que facilitam seu entendimento. Recomendado para uma visão geral da teoria quântica.)

[36] S. W. Golomb. “Perfect codes in the Lee metric and the packing of polyominoes, ” *SIAM J. Appl. Math.*, Vol 18, No. 2, January 1970.

[37] S. W. Golomb. *Polyominoes*. Princeton University Press, Princeton, New Jersey, (1994).

[38] D. Gottesman. “Class of quantum error-correcting codes saturating the quantum Hamming bound, ” *Physical Review A*, **54**, pp. 1862, (1996).

[39] D. Gottesman. “Stabilizer code and quantum error correction, ” *www.arxiv.org/abs/quant-ph/9705052*, (1997).

[40] D. Gottesman. “An introduction to quantum error correction, ” *www.arXiv.org/quant-ph/0004072*, (2000).

[41] D. Gottesman. *Stabilizer codes and quantum error correction*. Ph.D. Dissertation, California Institute of Technology Pasadena, California, (2002).

[42] J. L. Gross and T. W. Tucker. *Topological Graph Theory*, Dover Publications, INC, New York, (2001).

[43] L. K. Grover “A fast quantum mechanical algorithm for database search, ” *Proceedings of the 28th Annual Symposium on the Theory of Computing*, pp. 212, (1996).

[44] A. Hefez and M. L. T. Villela. *Códigos Corretores de Erros*. Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, Rio de Janeiro, (2002).

[45] T. Jørgensen and M. Näätänem. “Surface of genus 2: generic fundamental polygons, ” *Quart. J. Math. Oxford (2)*, **33**(1982), pp. 451–461, (1982).

[46] S. Katok. *Fuchsian Groups*. The University of Chicago Press, (1992).

[47] L. H. Kauffman and S. J. Lomonaco. “Braiding operators are universal quantum gates, ” *New Journal of Physics*, **6**, pp.134, (2004).

[48] A. Y. Kitaev. “Fault-tolerant quantum computation by anyons,” *Annals of Physics*, **303**, pp. 2–30, (2003).

[49] G. G. La Guardia. *Métodos de Construção de Códigos Quânticos CSS e Conexões entre Códigos Quânticos e Matróides*. Tese de doutorado, FEEC - UNICAMP, Campinas-SP, (2008).

[50] S. Lin and D. J. Costello Jr. *Error Control Coding*. Prentice-Hall, Inc. Englewood Cliffs, New Jersey, (1983).

[51] J. H. van Lint. *Coding Theory*. Springer-Verlag, Berlin, Heidelberg, (1973).

[52] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Bell Laboratories, Murray Hill, New Jersey, USA, (1977).

[53] G. Nakamura. "Generic fundamental polygons for surfaces of genus three, " *Kodai Math. J.*, **27**(2004), pp. 88–104, (2004).

[54] C. Nayak, S. H. Simon, A. Stern, M. Freedman and S. Das Sarma. "Non-abelian anyons and topological quantum computation, " *www.arXiv.org/quant-ph/0707.1889*, (2008).

[55] M. A. Nielsen. "Regras para um mundo quântico complexo, " *Scientific American Brasil*, dezembro, 80, (2002).

[56] M. A. Nielsen and I. L. Chuang. *Computação Quântica e Informação Quântica*. Bookman, (2003).

[57] T. P. Nóbrega Neto, J. C. Interlando, O. M. Favareto, M. Elia and R. Palazzo Jr. "Lattice Constellations and Codes from Quadratic Number Fields, " *IEEE Transactions on Information on Theory*, Vol. 47, No. 4, (2001).

[58] G. Nakamura. "Trace fields of genus 3 surfaces with regular fundamental polygons, " *Aichi Institute of Technology*, **1387** pp. 170–178, (2004). (www.kurims.kyoto-u.ac.jp/∼kyodo/kokyuroku/contents/pdf/1387-22.pdf)

[59] S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan and C. Monroe. "Quantum teleportation between distant matter qubits, " *Science*, **323**, pp. 486–489, (2009).

[60] D. Pengelley. "Self-dual orientable embeddings of K_n, " *J. Combin. Theory Ser. B*, 18, pp. 46–52, (1975).

[61] W. W. Peterson and E. J. Weldon Jr. *Error-Correcting Codes*. The Massachusetts Institute of Technology, (1984).

[62] J. Preskill. "Lectures notes for physics 219: quantum error correction, " *California Institute of Technology*, (1999).

[63] J. Preskill. “Lectures notes for physics 219: quantum computation, ” *California Institute of Technology*, (2004).

[64] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley Longman, (1994).

[65] P. Samuel. *Algebraic Theory of Numbers* Hermann, (1970).

[66] B. Schumacher. “Quantum coding, ” *Phys. Rev. A*, **51** pp. 2738–2747, (1995).

[67] A. Scott. “Os limites do computador quântico, ” *Scientific American Brasil*, **71** Ano 6, pp.56–63, (2008).

[68] C. E. Shannon. “A mathematical theory of communication, ” *The Bell System Technical Journal*, **27**, pp. 379–423, pp. 623–656 (1948).

[69] P. W. Shor “Algorithms for quantum computation: Discrete logarithms and factoring, ” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124, (1994).

[70] P. W. Shor. “Scheme for reducing decoherence in quantum memory, ” *Physical Review A*, **52**, pp. 2493, (1995).

[71] E. B. Silva, M. Firer, S. I. R. Costa and R. Palazzo Jr. “Signal constellations in the hyperbolic plane, ” *Journal the Franklin Institute*, **343**, pp. 69–82, (2006).

[72] A. M. Steane. “Multiple particle interference and quantum error correction, ” *Proc. R. Soc. Lond. A*, **452**, pp. 2551–2577, (1996).

[73] A. M. Steane. “Error correcting codes in quantum theory, ” *Phys. Rev. Letters*, **77**, pp. 793, (1996).

[74] A. M. Steane. “Simple quantum error correcting codes, ” *Physical Review Letters*, **77**, pp. 793–797, (1996).

[75] S. K. Stein and S. Szabó. *Algebra and Tiling: Homomorphisms in the Service of Geometry* The Mathematical Association of America, (1994).

[76] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat’s Last Theorem* A K Peters, (2002).

[77] J. Stillwell. *Geometry of Surfaces*. Springer-Verlag, (2000).

[78] C. C. Tannoudji, B. Diu and F. Laloë. *Quantum Mechanics - Volume One*. John Wiely and Sons, New York, (1977).

[79] V. L. Vieira. *Grupos Fuchsianos aritméticos identifcados em ordens dos quatêrnios para construção de constelações de sinais*. Tese de Doutorado, FEEC, Unicamp, (2006).

[80] C. Walkden. *Hyperbolic geometry*. www.maths.manchester.ac.uk/ cwalkden/hyperbolic-geometry/hyperbolic-geometry.html